«Jusan Bank» АҚ

Куәландырушы орталық қызметінің ҚАҒИДАЛАРЫ

Иесі:	Цифрлық дамыту департаменті	
Қосалқы иесі:		
Әзірлеуші:	Цифрлық дамыту департаменті	
Реттеу субъектілері:	Технологиялық шешімдер департаменті АЖ қолдау департаменті Сәулет шешімдері бөлімі Жүйелік қамтамасыз ету және телекоммуникация департаменті Ақпараттық жүйелерді қорғау департаменті	
Бекітілген:	Басқарма (№61-23 хаттама)	«02» маусым 2023ж.
Күші жойылды деп танылған ІҚ:	Куәландырушы орталық қызметінің қағидалары	"Jusan Bank" АҚ Басқармасымен бекітілген (21.04.2023 ж. № 43-23 хаттама)

Мазмұны

1-тарау. Жалпы ережелер

1. Осы куәландырушы орталық (бұдан әрі - КО) қызметінің қағидалары (бұдан әрі – Қағидалар) "Jusan Bank" АҚ куәландырушы орталығының жұмыс істеуін қамтамасыз ету және электрондық құжат және электрондық цифрлық қолтаңба мәселелері бойынша Қазақстан Республикасының (бұдан әрі – ҚР) заңнамасы[1] негізінде Банктің жеке тұлғаларына-клиенттеріне тіркеу куәлігін беру жөнінде қызметтер көрсету мақсатында әзірленді және оның жұмыс істеу тәртібін айқындайды.

2. Қағидалар RFC 3647 «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework» (x. 509 форматындағы ашық кілттердің интернет инфрақұрылымындағы сертификаттар саясаты мен практикасы құжаттарының құрылымы) халықаралық салалық ұсынымдарын ескере отырып әзірленді.

3. Қағидалар "Jusan Bank" АҚ куәландырушы орталығының тіркеу куәліктерін (бұдан әрі – тіркеу куәліктерінің саясаты/саясаты) қолдану саясатымен айқындалған сервистер жиынтығын қамтамасыз ету кезінде КО іске асыратын шараларды реттейді және тіркеу куәлігін шығарумен, басқарумен және кері қайтарып алумен шектелмейді.

4. Қағидалардың Саясаттан айырмашылығы, тәртіп пен процедураларды анықтайды:

1) КО функциясын (сервистердің жұмысын) орындау;

2) қауіпсіздікті қамтамасыз ету және ашық кілттер инфрақұрылымының өзегін басқару.

5. КО сервистерін пайдаланатын ақпараттық жүйеге қатысушы қол қойған сәттен бастап, қатысушы үшін тіркеу куәлік шығарға өтініш (бұдан әрі – өтініш) қол қойылған өтініште қамтылған осы Қағидалармен оған қолданылатын талаптарды орындауға міндетті болады.

6. Қағидалар сондай-ақ КО шығаратын тіркеу куәлігін шығаруға және одан әрі қызмет көрсетуге байланысты тексеру рәсімдерін айқындайды.

7. КО тіркеу куәлігі келесі мақсаттарға қолданылады:

1) электрондық құжаттарға (кредиттік шарттарға/өтініштерге) электрондық цифрлық қолтаңбамен қол қою;

2) электрондық цифрлық қолтаңбаны тексеру;

3) пайдаланушылардың аутентификациясы.

8. КО тіркеу куәліктерін пайдалану тәсілдері ҚР қолданыстағы заңнамасына және Қағидалардың талаптарына қайшы келмеуі тиіс.

9. КО шығаратын тіркеу куәліктері түрлерінің тізбесі олардың сәйкестендіретін белгілерін (профильдерін) көрсете отырып, төмендегі кестеде келтірілген:

Сипаттамасы	**Key Usage кеңейтімінің мәні**
Электрондық цифрлық қолтаңбаның көмегімен электрондық құжаттардың түпнұсқалығын, тұтастығын және дәлелділігін қамтамасыз ету үшін тіркеу куәліктері	c0 (OID 2.5.29.15 сәйкес)
Шифрлау арқылы кілттер мен деректердің құпиялылығын қамтамасыз ету үшін тіркеу куәліктері	38 (OID 2.5.29.15 сәйкес)

10. КО осы Қағидалар тарауына сәйкес әртүрлі мақсаттарға ие тіркеу куәлігін және тиісінше тіркеу куәлігінің "keyUsage" және/немесе "extendedKeyUsage" кеңейтілімінде көрсетілетін профильдерді шығарады.

11. "Cerificatepolicies"тіркеу куәлігін кеңейтуде тіркелетін Объектілік саясат идентификаторларының көмегімен тіркеу куәлігінің КО шығаратын рұқсат етілген қолдану саласы қосымша бөлінуі мүмкін.

---

[1] ҚР заңнамасы, оның ішінде электрондық құжат және электрондық цифрлық қолтаңба туралы ҚР Заңы; Дербес деректер және оларды қорғау туралы ҚР Заңы; Қазақстан Республикасы цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2020 жылғы 27 қазандағы № 405/НҚ бұйрығымен бекітілген куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін жасау, пайдалану және сақтау қағидалары; Қазақстан Республикасы Инвестициялар және даму министрінің 2015 жылғы 9 желтоқсандағы № 1187 бұйрығымен бекітілген электрондық цифрлық қолтаңбаның түпнұсқалығын тексеру қағидалары

12. Саясаттың Объектілік идентификаторына мынадай КО қызметкерлері кіреді:

1) КО әкімшісі - АЖ қолдау департаментінің мынадай функцияларды орындайтын қызметкері: шаблондарды әзірлеу (КО бизнес иесінің талабы бойынша қосымшада конфигурацияны баптау), куәлікті шығаруды қайта тіркеу, сертификаттау орталығының жұмыс істеуін қамтамасыз ететін Сертификаттау орталығының жұмысын тексеру;

2) КО жүйелік әкімшісі - жүйелік қамтамасыз ету және телекоммуникация департаментінің бақылайтын/қызмет көрсететін/орындайтын функцияларды орындайтын қызметкері: консоль, желі, деректер базасы, HSM іске қосуды сүйемелдеу, құзырет шеңберінде ақаулыққа төзімділікті қамтамасыз ету, КО серверлеріне қолжетімділікті қамтамасыз ету, HSM бэкап;

3) КО қауіпсіздік офицері - токендерді сақтау функциясын орындайтын Ақпараттық жүйелерді қорғау Департаментінің қызметкері;

4) КО бастығы - КО бизнес-иесі, қағиданы, саясатты, бұйрықтарды әзірлеу, Банк қызметкерлеріне рұқсат беруді келісу, жанжалды жағдайларды талдау функцияларын орындайтын Цифрлық дамыту департаментінің қызметкері;

5) КО кезекшісі - КО сертификаттау орталығының / бағдарламалық қамтамасыз ету мониторингі бойынша функцияларды орындайтын Жүйелік қамтамасыз ету және телекоммуникация департаментінің қызметкері.

13. Клиенттік тіркеу куәлігіндегі объектілік саясат идентификаторларының толық тізбесі Банктің ресми ақпараттық ресурсында (корпоративтік интернет ресурс) келтірілген.

14. Криптографиялық кілттер жұбын пайдаланудың бекітілген мақсаты қатысушы үшін КО шығарған әрбір тіркеу куәлігінде "keyUsage" және/немесе "extendedKeyUsage" кеңейтімінде тіркеледі.

15. Объектілік саясат идентификаторларының болуы тіркеу куәлігін пайдаланатын ақпараттық жүйелерге жарамсыз тіркеу куәлігін қолдануды шектей отырып, қажетті және тыйым салынған саясаттар жиынтығының жүйесін бақылау нысанында қосымша қорғау мүмкіндігін береді.

2-тарау. Глоссарий

16. Қағидада келесі негізгі ұғымдар, анықтамалар мен қысқартулар қолданылады:

1) аутентификация - әртүрлі параметрлердің, оның ішінде парольдерді немесе аутентификациялық белгілерді (цифрлық сертификаттар, токендер, смарт-карталар, бір реттік пароль генераторлары және биометриялық сәйкестендіру құралдары) жасау мен енгізудің комбинациясы арқылы пайдаланушының түпнұсқалығын тексеру тәсілі;

2) Банк – «Jusan Bank» АҚ;

3) КО бизнес-иесі - тіркеу куәлігін шығару бойынша КО негізгі бизнес-процесінің иесі болып табылатын Банктің бөлімшесі;

4) АЖ бизнес-иесі – Банктің фронтальды жүйесінің (Jusan, jusan Business мобильді қосымшасы және басқалары)/тіркеу орталығының бизнес-процесінің иесі болып табылатын Банктің бөлімшесі. Тіркеу орталығына өзгерістер/пысықтаулар енгізу қажет болған жағдайда АЖ бизнес-иесі ақпараттық жүйелерді, кіші жүйелерді, модульдерді әзірлеу, пысықтау және енгізу кезіндегі өзара іс-қимыл тәртібін регламенттейтін ІҚ-ға сәйкес осы жүйені техникалық қолдауға жауапты Банк бөлімшесіне жүгінеді;

5) блокчейн - өзара байланысты деректер блоктарының тізбегі, берілген тұтастықты растау алгоритмдері және шифрлау құралдары негізінде таратылған деректер платформасындағы ақпараттың өзгермейтіндігін қамтамасыз ететін ақпараттық-коммуникациялық технология;

6) ІҚ – Банктің ішкі құжаттары;

7) тіркеу куәлігінің иесі - атына тіркеу куәлігінде көрсетілген ашық кілтке сәйкес келетін жабық кілтті заңды түрде иеленетін тіркеу куәлігі берілген жеке тұлға;

8) белсендендіру деректері -криптографиялық операцияларды орындау үшін қажетті және қорғауды талап ететін кілттерді қоспағанда, кез келген деректер: дербес сәйкестендіру

нөмірлері (PIN), құпия сөз тіркестері, бөлінген кілт компоненттері, биометриялық параметрлер және басқалар;

9) сенім білдіруші тарап - КО шығарған тіркеу куәлігі туралы алынған мәліметтерді ҚР түбірлік КО, Банк порталы, КО тіркеу куәліктерін пайдаланатын мемлекеттік ақпараттық жүйелер арқылы иесіне ЭЦҚ тиесілігін тексеру үшін пайдаланатын тіркеу куәлігін пайдаланушы;

10) халықаралық объектілік сәйкестендіргіштер ағашы - стандартталған ITU-T және ISO/IEC (X. 660) кез келген нақты немесе дерексіз объектілерді бір типті, бір мағыналы, жан-жақты атаулармен атау механизмі, үш ерекше пішінді иерархиялық ағаштарды (3 түрлі тамырдан) пайдаланып атауларды тіркеуге арналған, онда әрбір келесі түйін бүтін санға ие және одан шығатын тармақтарды одан әрі бөлуге және тіркеуге жауапты;

11) электрондық цифрлық қолтаңбаның жабық кілті (ЭЦҚ жабық кілті) – электрондық цифрлық қолтаңба құралдарын пайдалана отырып, электрондық цифрлық қолтаңбаны жасауға арналған электрондық цифрлық нышандар тізбегі;

12) сәйкестендіру – Қағида мәтінінде, жеке тұлғаның жеке басын анықтайтын процесс (немесе процестің нәтижесі) (берілген тұлғаның белгілі бір нақты тұлға екенін көрсететін) және екі кезеңнен тұрады:

а) тұлға ұсынған атаудың тұлғаның нақты бар бірдейлігінің сәйкестігін анықтау;

б) бір нәрсеге қол жеткізу үшін белгілі бір атауы бар тұлғаның шын мәнінде солай аталатын (аутентификация) тұлға екенін анықтау;

13) ашық кілттер инфрақұрылымы (АКИ) – ашық кілттермен криптожүйелер негізінде криптографиялық міндеттерді (аутентификация, шифрлау, тұтастық пен дәлелділікті бақылау) шешу үшін жиынтықта пайдаланылатын, аталған міндеттер шешілетін ашық кілттерді басқаруды дербес қамтамасыз етуге қабілетті құралдар (техникалық, материалдық, адамдық және өзге де), бөлінген қызметтер мен компоненттер жиынтығы;

14) ақпараттық жүйе (АЖ) – ақпараттық өзара іс-қимыл арқылы белгілі бір технологиялық әрекеттерді іске асыратын және нақты функционалдық міндеттерді шешуге арналған ақпараттық-коммуникациялық технологиялардың, қызмет көрсететін персоналдың және техникалық құжаттаманың ұйымдық-реттелген жиынтығы, тіркеу орталығы;

15) жабық кілттерді бұзу - жабық кілттер иесінің нақты жабық кілттер олардың көмегімен қорғалатын ақпараттың қауіпсіздігін қамтамасыз ететініне деген сенімін жоғалту;

16) негізгі ақпарат тасығыш - электрондық цифрлық қолтаңбаның сақталған жабық кілттерін қорғау үшін ҚР заңнамасының талаптарына сәйкестік сертификаты бар ақпаратты криптографиялық қорғау құралдары пайдаланылатын мамандандырылған тасығыш;

17) нысан идентификаторы - бұл объектімен байланысқан және оны объектілердің әлемдік мекен-жай кеңістігінде бірегей түрде анықтайтын сандардың бірегей жиынтығы;

18) электрондық цифрлық қолтаңбаның ашық кілті (ЭЦҚ ашық кілті) - кез келген тұлғаға қолжетімді және электрондық құжаттағы электрондық цифрлық қолтаңбаның түпнұсқалығын растауға арналған электрондық цифрлық символдардың реттілігі;

19) хэш - еркін ұзындықтағы кіріс деректерінің массивін бекітілген ұзындықтың биттік жағына түрлендіру;

20) Тіркеу куәліктерін қолдану саясаты (тіркеу куәліктерінің саясаты/саясаты деп те аталады) – ақпараттық қауіпсіздіктің жалпы талаптары бар қосымшалардың белгілі бір қауымдастығында (класында) тіркеу куәлігінің қолданылуын анықтайтын ережелердің жиынтығы;

21) Куәландырушы орталық қызметінің қағидалары (қағидалары) - саясатқа сәйкес жүзеге асырылатын КО-ның негізгі қызметін ұйымдастыру тәртібін айқындайтын ІҚ;

22) тіркеу куәлігі - "электрондық құжат және электрондық цифрлық қолтаңба туралы" ҚР Заңында белгіленген талаптарға электрондық цифрлық қолтаңбаның сәйкестігін растау үшін КО беретін электрондық құжат;

23) қайтарып алынған тіркеу куәліктерінің тізімі (ҚТКТ) – қолданысы тоқтатылған тіркеу куәліктері туралы мәліметтерді, олардың сериялық нөмірлерін, кері қайтарып алу күні

мен себебін қамтитын тіркеу куәліктері тіркелімінің бөлігі;

24) ақпаратты криптографиялық қорғау құралдары (АККҚ) – криптографиялық түрлендіру, кілттерді құру, қалыптастыру, тарату немесе басқару алгоритмдерін жүзеге асыратын құралдар;

25) электрондық цифрлық қолтаңба құралдары (ЭЦҚ құралдары) – электрондық цифрлық қолтаңбаны жасау және оның түпнұсқалығын тексеру үшін пайдаланылатын бағдарламалық және техникалық құралдардың жиынтығы (электрондық цифрлық қолтаңба құралдары ақпаратты криптографиялық қорғау құралдарының бір түрі болып табылады);

26) токен - Қағида контекстінде, жабық кілттердің резервтік көшірмесін және КО аппараттық криптографиялық модульдерінің (Hardware security Module, HSM) параметрлерін қорғалған сақтауды ұйымдастыру мақсатында уәкілетті тұлғаға берілетін жеке құрылғы;

27) ашық кілттер инфрақұрылымына қатысушылар (АКИ қатысушысы) – клиенттерге қызмет көрсетуге жауапты КО қызметкерлері, сондай-ақ тіркеу куәліктерінің иелері;

28) Куәландырушы орталық (КО) - электрондық цифрлық қолтаңбаның ашық кілтінің электрондық цифрлық қолтаңбаның жабық кілтіне сәйкестігін куәландыратын, сондай-ақ тіркеу куәлігінің дұрыстығын растайтын Банк;

29) сертификаттау орталығы - тіркеу куәлігін беруге, қызмет көрсетуге және кері қайтарып алуға арналған КО бағдарламалық-аппараттық кешені, ҚР заңнамасына сәйкес әрекет ететін ҚТКТ уақтылы импорты. Сертификаттау орталығының сервисі қолжетімсіз болған жағдайда КО тіркеу куәліктерін шығару жүзеге асырылмайды;

30) тіркеу орталығы - иесінен тіркеу куәлігін шығаруға және кері қайтарып алуға өтініштерді қабылдайтын, сондай-ақ өтініш берушілерді тексеруді, сәйкестендіруді және аутентификациялауды жүзеге асыратын банктің фронтальды жүйесі (Juan мобильді қосымшасы);

31) тіркеу куәліктерінің тізбегі – тіркеу куәлігінен басталатын тіркеу куәліктерінің реттелген реттілігі, онда электрондық цифрлық қолтаңба сенімді түбірлік тіркеу куәлігінің көмегімен тексерілуі мүмкін, оны стандартталған алгоритмнің көмегімен сәтті өңдеу "subject"өрісінде тізбектің қорытынды тіркеу куәлігінде көрсетілген тұлғаға ашық кілттің тиесілігін растауға мүмкіндік береді;

32) электрондық цифрлық қолтаңба (ЭЦҚ) – электрондық цифрлық қолтаңба құралдарымен жасалған және электрондық құжаттың дұрыстығын, оның тиесілілігін және мазмұнының өзгермейтіндігін растайтын электрондық цифрлық нышандар жиынтығы;

33) электрондық құжат - ақпарат электрондық-цифрлық нысанда ұсынылған және ЭЦҚ арқылы куәландырылған құжат.

Қағида мәтіні бойынша пайдаланылатын өзге де терминдер мен қысқартулар ҚР заңнамасында, жалпы банктік глоссарийде бекітілген мәнге сәйкес, ал олар болмаған кезде ҚР заңнамасында және жалпы банктік глоссарийде – халықаралық банк практикасында бекітілген мәнге сәйкес қолданылады.

Құжат атауын көрсетпей саясат мәтініндегі бөлімдерге, бөлімдерге, тарауларға, абзацтарға, тармақтарға, қосымшаларға барлық сілтемелер осы Қағидаға жатады.

3-тарау. Деректерді сақтау және жариялау (тіркеу куәлігі)

§1. Сақтау орны

17. КО Банктің ресми ақпараттық ресурсында (корпоративтік интернет-ресурс) тіркеу куәлігін шығару және ҚТКТ орналастыру туралы меншік иелері мен сенімді тараптарды хабардар ету мақсатында, сондай-ақ Саясатқа сәйкес жариялайды:

1) Политику регистрационных свидетельств;

2) Қағида;

3) КО тіркеу куәліктері;

4) ҚТКТ-ға қол жеткізу үшін сілтемелер.

18. Тіркеу куәлігін шығару және ҚТКТ орналастыру туралы меншік иелері мен сенім білдірілген тараптардың КО-ның ресми хабарламасы Банктің корпоративтік интернет-ресурсы

арқылы қолжетімді сақтау орнында жариялау, сондай-ақ оны тіркеу орталығында сақтау болып табылады. Қосымша Банктің корпоративтік интернет-ресурсы тіркеу куәліктерінің иелері мен пайдаланушыларын (меншік иелері мен сенім білдіруші тараптарды) хабардар ету мақсатында КО-ның өзге де маңызды ақпаратын орналастыру үшін пайдаланылады.

§2. Тіркеу куәліктері туралы ақпаратты сақтау орнында жариялау

19. КО сақтау орнымен ақпараттық өзара іс-қимылдың негізгі хаттамасы RFC 2251 (Lightweight directory Access Protocol v. 3, 3-нұсқа) ұсыныстарымен анықталған нұсқадағы каталогтарға қол жеткізудің жеңілдетілген хаттамасы болып табылады.

20. Бұл хаттама тіркеу куәліктерінің болуы туралы сұраулармен КО қоймасына онлайн режимінде жүгінуге және олардың мазмұнын алуға мүмкіндік береді.

21. Осы талаптардан кез келген ерекшеліктер, олар туындаған жағдайда, Қағидаға енгізілуі және тіркеу куәліктерінің иелері мен пайдаланушыларының (меншік иелері мен сенім білдіруші тараптардың) еркін қол жеткізуінде жариялануы тиіс.

22. КО қоймасында онлайн режимде барлық қолданыстағы тіркеу куәліктері ("кері қайтарып алынды" мәртебесі жоқ валидті тіркеу куәліктері), сондай-ақ ҚТКТ жарияланады.

§3. Сақтаудағы деректерді өзектілендіру кезеңділігі

23. КО шығарған әрбір тіркеу куәлігі сақтау орнына енгізіледі және автоматты түрде және дереу жарияланады (онлайн режимінде).

24. Иеленушінің жабық кілтінің қолданылу кезеңінің басталуы тиісті тіркеу куәлігінің қолданысы басталған күн мен уақыттан бастап есептеледі.

25. КО тіркеу куәліктерінің қолданылу мерзімі:

1) түбірлік тіркеу куәлігі берілген сәттен бастап – 20 (жиырма) жыл;

2) жабық кілттері КО-да сақталатын тіркеу куәлігі берілген сәттен бастап - 1 (бір) жыл.

26. Сақтау орнында орналастырылған барлық тіркеу куәліктерінің қолданылу мерзімінің аяқталуын тексеру КО АЖ-нің тиісті баптауымен айқындалған кесте бойынша тәулік сайын автоматты түрде жүзеге асырылады.

27. 27. КО кері қайтарып алған кезде тіркеу куәлігі автоматты түрде қоймадан шығарылады және ҚР заңнамасының талаптарына сәйкес сақталатын мұрағатқа көшіріледі.

28. Қайтарып алынбаған, бірақ жарамдылық мерзімінің аяқталуына байланысты қолданысын тоқтатқан тіркеу куәліктері автоматты түрде қоймадан шығарылады және мұрағатқа көшіріледі.

29. Қолданылу мерзімі өткен кері қайтарып алынған тіркеу куәліктері туралы мәліметтер сертификаттау орталығының тиісті баптауымен айқындалған кесте бойынша аптасына кемінде бір рет тіркеу куәлігінің қолданылу мерзімінің аяқталу фактісі бойынша кері қайтарып алынған тіркеу куәліктерінің тізімінен жойылады.

30. Кез келген тіркеу куәлігі қайтарып алынған жағдайда КО автоматты түрде және дереу онлайн режимінде жаңартылған ҚТКТ қалыптастырады және сақтау орнында жариялайды.

31. Тіркеу куәліктерін кері қайтарып алу оқиғалары болмаған жағдайда, жаңа ҚТКТ сертификаттау орталығының тиісті баптауымен айқындалған кесте бойынша апта сайынғы негізде қалыптастырылады және автоматты түрде шығарылады.

32. Кері қайтарып алынған тіркеу куәліктерін сақтау мерзімі кемінде 5 (бес) жылды құрайды. Мерзімі өткеннен кейін кері қайтарып алынған тіркеу куәліктері мұрағатқа түседі.

§4. Сақтау орнына кіруді басқару

33. Қоймадан деректерді оқу үшін қол жетімділікті бақылау және басқару жүйелерін монтаждау және орналастыру қағидалары туралы ІҚ белгілеген тәртіппен өтінімдер бойынша банктің қызмет көрсетілетін АЖ-ға КО береді.

34. Қол жеткізу матрицасына сәйкес КО әкімшісіне, КО жүйелік әкімшісіне уәкілетті тұлғалардың шектеулі тобы үшін КО-ға деректерді қосу, өзгерту (жою) үшін қолжетімділік беріледі.

35. КО қоймаға рұқсатсыз кіруден қорғауды жүзеге асырады. Банктің корпоративтік интернет-ресурсында жарияланатын мәліметтер АКИ қатысушыларына "тек оқу үшін" құқықтарымен еркін қол жеткізу режимінде ұсынылады.

36. Қызмет көрсету деңгейінің тиісті параметрлерін сақтау сақтау орнына кіру сервисіне жүктеме артқан жағдайда КО кибершабуылдарға, сервистерді берудегі іркілістің өзге де қатерлеріне қарсы іс-қимылдың белсенді шаралары ретінде қолжетімділіктің уақытша шектеулерін автоматты түрде қолданады.

37. Кибершабуылдар, сервистерді берудегі іркілістің өзге де қатерлері немесе оларда негізделген күдік болған жағдайларда КО белсенді қарсы іс-қимыл шаралары ретінде қоймадан деректерді оқу үшін қолжетімділіктің уақытша шектеулерін қолдану құқығын өзіне қалдырады.

4-тарау. Тіркеу куәліктерінің иелерін сәйкестендіру және аутентификациялау

§1. Атауларға қойылатын талаптар

38. КО пайдаланатын субъектілерді атау қағидалары барлық шығарылатын тіркеу куәліктері бойынша тіркеу куәліктерінің иелерін (иелерін) сәйкестендіруді қамтамасыз етеді.

39. Тіркеу куәліктерінің резидент-иелерін сәйкестендіру ЖСН сәйкестендіру нөмірлерін пайдалану есебінен қол жеткізіледі.

40. Резидент емес жеке тұлғаны сәйкестендіруге нөмір және паспорттың басқа деректері есебінен қол жеткізіледі.

41. Тіркеу куәліктері иелерінің анонимділігіне жол берілмейді.

42. Тіркеу куәліктерінің иелерінің жалпыға белгілі атаулардың орнына бүркеншік атаулар пайдалануына жол берілмейді.

43. Тіркеу куәлгін шығаруға өтініш берушілер өздерінің өтініштерінде заңды құқық иелерінің құқықтарын бұзатын есімдерді пайдаланбауға тиіс.

44. Тіркеу орталығы, егер оған дұрыс емес ақпаратты ұсыну фактісі туралы белгілі болса, тіркеу куәлік шығарға кез келген өтінішті қабылдамау құқығын өзіне қалдырады.

45. КО шығаратын барлық тіркеу куәліктерінде субъектілердің атаулары ITU-T X. 520 халықаралық ұсынымдарына сәйкес "Issuer" және "Subject" жолдарында бөлінген атаулар (DN-атаулар) форматында көрсетіледі.

46. КО түбірлік тіркеу куәлігінің "Issuer" және "Subject" өрістерінің атрибуттары мен мазмұны төмендегі кестеде келтірілген:

Атрибут	**Мәні**
Country (C=)	KZ
Organization (O=)	Jusan Bank JSC
Common Name (CN=)	Certification Authority

47. "Subject" өрісіндегі КО түбірлік тіркеу куәлігінде "Issuer" жолындағыдау дәл деректер бар.

48. КО шығаратын барлық түбірсіз тіркеу куәліктерінің "Issuer" өрісіне түбірлік тіркеу куәлігінің "Issuer" жолындағыдай атрибуттар мен мәндер дәл енгізіледі.

49. Меншік иелерінің тіркеу куәліктеріне "Subject" жолында атрибуттар жиынтығы енгізіледі, ол төмендегі кестеде келтірілген:

Атрибут	**Мәні**
Country (C=)	KZ
Organization (O=)	Jusan Bank JSC
Organization unit (OU=)	*Банктің логикалық немесе құрылымдық бірлігі, мысалы, Банктің ақпараттық жүйесі, оның ішкі жүйесі, блогы, департаменті немесе Банктің басқа бөлімшесі*

[Common name (CN=)	*Тіркеу куәлігі иесінің коды (ТАӘ)*
Unique identification number (UID=)	*Тіркеу куәлігі иесінің коды (ЖСН)*

50. Бір мәнді сәйкестендіру мақсатында тіркеу куәліктерінің барлық иелерінің есімдері бірегей болып табылады.

§2. Бастапқы иесінің жеке басын тексеру

51. Бастапқы иесінің жеке басын тексеру – это наиболее полная форма процедур идентификации и аутентификации, которая согласно международным отраслевым рекомендациям проводится в отношении владельца при выпуске первого регистрационного свидетельства.

52. Тіркеу орталығы ақпараттандыру саласындағы уәкілетті орган шығарған тіркеу куәліктерін беру, сақтау, кері қайтарып алу мәселелері бойынша ҚР құқықтық актісіне (бұдан әрі – реттеушінің құқықтық актісі)сәйкес иесінің сәйкестігіне бастапқы тексеруді жүргізеді[2].

53. КО ЭЦҚ ашық кілтінің тиесілілігі мен жарамдылығын растауды АКИ қатысушылары арасында электрондық құжаттармен алмасу кезінде АКИ/ АЖ қатысушысы жүзеге асырады.

54. АКИ/АЖ қатысушысы қол қоюшы тараптың тіркеу куәліктері бар электрондық құжатты алған кезде ЭЦҚ ашық кілтінің тиесілігін және жарамдылығын растау үшін оны тексеруді жүзеге асырады:

1) қол қоюшы тараптың тіркеу куәлігін тексеру;

2) электрондық құжатта ЭЦҚ тексеру.

5-тарау. Тіркеу куәліктерінің өмірлік цикліне қойылатын операциялық талаптар

§1. Тіркеу куәлігін шығаруға (беруге) өтініш

55. Тіркеу орталығы дербес әрекет ететін жеке тұлғалардан тіркеу куәлігін шығаруға өтініш қабылдайды.

56. Өтініш берушінің тіркеу куәлігін шығаруға (беруге) өтініші тіркеу орталығында реттеушінің құқықтық актісіне сәйкес нысан бойынша беріледі.

57. Иесіне тіркеу куәлігін беруді тіркеу орталығы жүзеге асырады.

58. КО берген иесінің тіркеу куәлігі және КО тіркеу куәлігі X. 509 стандартының талаптарына және RFC 5280 стандартының ұсынымдарына сәйкес болуы тиіс.

59. Өтініш берушіге тіркеу куәлігін беру реттеушінің құқықтық актісіне сәйкес нысан бойынша тіркеу куәлігінің құрылымымен электрондық құжат нысанында жүзеге асырылады.

60. КО өзінің атауын өзі шығарған әрбір тіркеу куәлігіне, ҚТКТ-қа қосады және оларға ЭЦҚ-ның жеке жабық кілтінің көмегімен қол қояды.

61. Тіркеу куәліктерін беру кезінде осы тіркеу куәлігіне КО ЭЦҚ қол қойылады.

62. Тіркеу куәлігін шығаруға арналған өтініште Саясат пен Қағидаларға сілтеме бар.

63. Тіркеу куәлігін шығаруға арналған өтініш өтініш берушінің тіркеу куәліктерінің иесі мен пайдаланушысының (меншік иесі мен сенім білдіруші Тараптың) қағидаттарды сақтау және Саясат пен Қағидалардың талаптарын орындау міндеттемелерін қабылдауын білдіретін құжат болып табылады.

64. Тіркеу куәліктерінің иесі мен пайдаланушысының (меншік иесі мен сенім білдіруші тараптың) қажетті КО міндеттемелері Қағидалардың 10-тарауының 4-параграфында ("кепіл мен растамалар") баяндалған.

---

[2] Қазақстан Республикасы Инвестициялар және даму министрінің 2015 жылғы 23 желтоқсандағы № 1231 бұйрығымен бекітілген Қазақстан Республикасының түбірлік куәландырушы орталығын, Мемлекеттік органдардың куәландырушы орталығын, Қазақстан Республикасының Ұлттық куәландырушы орталығын және Қазақстан Республикасының сенім білдірілген үшінші тарабын қоспағанда, куәландырушы орталықтың тіркеу куәліктерін беру, сақтау, кері қайтарып алу және электрондық цифрлық қолтаңбаның ашық кілтінің тиесілілігі мен жарамдылығын растау қағидалары

§2. Тіркеу куәліктерін шығаруға өтініштерді өңдеу

65. Тіркеу куәлігін шығаруға өтініш беру тіркеу орталығы арқылы жүзеге асырылады.

66. Сұрау салу процесінде өтініш беруші:

1) дербес деректерді жинауға және өңдеуге келісім беру;

2) биометриялық аутентификацияны қоса, аутентификация процедурасынан өтіңіз;

3) КО HSM қауіпсіздік модулінде бұлтты ЭЦҚ жабық кілтін сақтауға келісім беру. Жасалғаннан кейін ЭЦҚ-ның жабық кілті HSM-де шифрланған түрде сақталады. Құпия мәндер ретінде құпия сөз қолданылады, ол КО - да сақталмайды.

67. КО өтініш беруші сәйкестендіру және аутентификация рәсімдерінен сәтті өткен жағдайда тіркеу куәлігін береді.

68. Тіркеу орталығы өтініш беруші өтініш берген кезде белгіленген мерзімде сәйкестендіру және аутентификациялау рәсімінен сәтті өтпеген жағдайда өтініш беруші өтініш берген күні құжаттарды қабылдаудан бас тартады.

69. Көрсетілген негіздер бойынша қабылданбаған тіркеу куәлігін шығаруға тіркелген барлық өтініштер белгіленген мерзімде қанағаттандырылуға жатады.

70. Тіркеу куәліктерін шығаруға өтінішті тіркеу орталығымен кері қайтарылуы мүмкін, егер:

1) өтініш беруші онда реттеушінің құқықтық актісіне сәйкес қажетті барлық ақпаратты көрсетпеді;

2) өтініш беруші оларда дұрыс емес мәліметтерді көрсетті;

3) заңды күшіне енген сот шешіміне сәйкес;

4) өтініш беруші 16 (Он алты) жасқа толмаған;

5) ҚР заңнамасында белгіленген өзге де жағдайларда.

71. ҚР заңнамасында белгіленген тіркеу куәлігін беруден бас тарту негіздерінің тізбесі өзгерген жағдайда ҚР қолданыстағы заңнамасының талаптары қолданылады. Қағидалар ҚР қолданыстағы заңнамасына сәйкес белгіленген тәртіпке келтірілуі тиіс.

72. Тіркеу куәліктерін шығаруға арналған өтініштерді КО жалпы алғанда өтініш тіркелген күннен бастап 5 (бес) жұмыс күнінен аспайтын мерзімде қарайды.

§3. Тіркеу куәлігін шығару

73. Тіркеу куәлігін шығару үшін өтініш беруші келесі кезеңдерден өтуі керек:

1) өтініш берушінің жеке басын сәйкестендіру;

2) сертификаттау орталығында негізгі жұптың қорғалған генерациясы;

3) өтініш берушіге ашық кілтті қорғалған жеткізу; КО тіркеуге жататын ашық кілтке сәйкес келетін жабық кілтті иелену фактісін тексеру.

74. Тіркеу куәлігін шығару кезінде КО сәйкестендіру және аутентификация рәсімдері барысында тіркеу орталығы сәтті тексерген өтініштен алынған ақпаратқа негізделеді.

75. КО шығарған кез келген тіркеу куәлігі автоматты түрде сақтау орнында жарияланады.

76. Тіркеу куәлігі иесінің ашық кілтін сертификаттау орталығынан тіркеу орталығына жеткізу қажет болған жағдайда оны ауыстырудан немесе бұрмалаудан қорғауға ЭЦҚ тетігін пайдалану есебінен қол жеткізіледі. Ашық кілт PKCS № 10 форматында жасалған және жабық кілтпен қол қойылған тіркеу куәлігін шығару туралы сұрау контекстіне енгізіледі.

77. Өтініш берушінің жабық кілтті иелену фактісі сұрауды өңдеу кезінде сертификаттау орталығы анықтайтын PKCS#10 форматындағы электрондық сұрау салуда ЭЦҚ болуы болып табылады.

78. Тіркеу орталығының, сертификаттау орталығының сервистері қолжетімсіз болған кезде КО тіркеу куәліктерін шығару (беру) жүзеге асырылмайды.

§4. Тіркеу куәлігі мен негізгі жұптарды пайдалану

79. КО шығарған тіркеу куәлігіне сенім негізінде кез келген актіні қабылдамас бұрын, сенім білдіруші тарап әрбір тиісті электрондық құжатты, атап айтқанда, ондағы әрбір ЭЦҚ-ны, сондай-ақ соған байланысты тіркеу куәліктерін, уақыт белгілерін, түбіртектерді (қызметтің жауаптарын) OCSP немесе ҚТКТ-ты дербес тексереді.

80. Жабық кілтті тіркеу куәлігінің иесі саясатқа сәйкес меншік иесі мен сенімді тараптың міндеттерін орындауға жазбаша міндеттеме бергеннен кейін ғана пайдаланады, КО тиісті ашық кілттің тіркеу куәлігін шығарды және иесі осы тіркеу куәлігін қабылдады.

81. Жабық кілтті пайдалану тиісті тіркеу куәлігіндегі "keyUsage" және "extendedKeyUsage" кеңейтімдерінің мазмұнына сәйкес келуі керек.

82. Жабық кілтті меншік иесі тек реттеушінің құқықтық актісіне, шарттық міндеттемелерге, Саясатқа және Қағидаларға сәйкес пайдаланады.

83. ЭЦҚ тексеруді жүргізу үшін тіркеу куәлігін пайдаланушы (сенім білдіруші тарап) мынадай әрекеттерді орындайды:

1) ЭЦҚ қалыптастырған субъектіні анықтауға мүмкіндік беретін тіркеу куәліктерінің тізбегін анықтайды және тексереді. Тіркеу куәліктерінің тізбегін тексеру барысында RFC 3280 "Internet X. 509 Public key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (сертификат профилі және X. 509 форматындағы ашық кілттер интернет инфрақұрылымының кері қайтарып алынған сертификаттар тізімі)ұсынымдарында баяндалған алгоритм пайдаланылады;

2) тізбектің әрбір тіркеу куәлігін тексеру барысында " keyUsage "және" extendedKeyUsage "кеңейтімдерінің пайдалану мақсатына сәйкестігін қосымша бақылайды;

3) қол қойған адамның электрондық құжатқа қол қою үшін жеткілікті өкілеттіктерінің болуын дербес тексереді. Сертификаттау орталығы өкілеттіктерді бақылау қызметін ұсынбайды.

84. Егер тексеру қадамдарының бірі теріс нәтиже берсе немесе оны орындау мүмкін болмаса, онда пайдаланушы (сенім білдіруші тарап) ЭЦҚ жарамсыз деп санайды және электрондық құжатты қабылдамайды.

85. Егер электрондық құжатта КО қалыптастырған уақыт белгісі болса, онда уақыт белгісіне сенімділікті талап ететін іс-әрекетті орындау үшін сенім білдіруші тарап электрондық құжаттағы ЭЦҚ тексеруге ұқсас тәртіппен де осы уақыт белгісін тексереді.

86. Егер тізбектің тіркеу куәліктерінің кез келгені ЭЦҚ тексеру сәтінде "кері қайтарып алынды" мәртебесіне ие болса, тек қана сенуші тарап тізбектің тіркеу куәліктерінің бірі кері қайтарып алынғанға дейін иесі қалыптастырған электрондық құжатқа сүйенудің негізделгенін немесе негізделмегенін өз тәуекеліне ғана шешеді. Мұндай жағдайларда КО тіркеу куәліктерін пайдаланушылар (сенім білдіруші тараптар) алдында жауапты болмайды, өйткені тіркеу куәлігін қайтарып алуға өтініш беру тіркеу куәлігінің нақты иесінің міндеті болып табылады.

87. Егер мән-жайлар электрондық құжат авторлары тарапынан қосымша кепілдіктердің қажеттігін көрсетсе, онда тіркеу куәлігін пайдаланушы (сенім білдіруші тарап) тіркеу куәліктерінің иелерінен тіркеу куәлігіне сенімділікті талап ететін әрекеттерді орындағанға дейін және КО-ға жүгінбей-ақ, осындай қосымша кепілдіктерді (растайтын құжаттарды) дербес алады.

88. Егер тіркеу куәлігін пайдаланушы (сенім білдіруші тарап) КО шығарған тіркеу куәлігіне сенімге негізделген кез келген актіні қабылдай отырып, Қағидалардың жоғарыда аталған талаптарын орындамаса, онда КО мұндай актінің салдары үшін сенім білдіруші тараптың алдында жауап бермейді. КО тіркеу куәліктерінде қолданылу мерзімдерін жаңарту бойынша қызметтерді ұсынбайды.

§5. Тіркеу куәлігіндегі кілттерді ауыстыру

89. Кілттерді ауыстыру және қажет болған жағдайда кілттердің болуын талап ететін Сертификаттау орталығының сервистерін одан әрі пайдалану үшін тіркеу куәлігінің иесі Қағидаларда айқындалған тәртіппен (жаңа) тіркеу куәлігін шығару рәсімінен қайта өтеді.

90. Кілттерді ауыстыру-жаңа жабық кілтті және оған сәйкес тіркеу куәлігін жасауды білдіреді. Кілттерді ауыстыру кезінде өтініш беру және тіркеу куәлігін беру рәсімі тіркеу куәлігін шығаруға (беруге) өтініш беру және оны өңдеу рәсімдеріне толығымен ұқсас.

91. Егер тіркеу куәлігінің қолданылу мерзімі аяқталғанға дейін күнтізбелік 30 (отыз) күннен аз уақыт қалса, кілттер мен тіркеу куәлігін меншік иесі дербес ауыстыра алады.

92. Тіркеу куәлігінің қолданылу мерзімі аяқталғанға дейін кілттерді ауыстыру иесінің қолданыстағы тіркеу куәлігіне сәйкес келетін жабық кілтпен қол қойылған сұрау салу берілген кезде орындалуы мүмкін.

93. Жаңа тіркеу куәлігін шығару үшін алдымен тіркеу куәлігін қайтарып алуға өтініш береді, содан кейін жаңасын шығаруға өтініш береді.

§6. Тіркеу куәлігіндегі деректерді өзгерту

94. КО тіркеу куәлігінде деректерді өзгерту бойынша қызметтерді ұсынбайды.

95. Тіркеу куәлігіндегі деректерді өзгерту үшін оның иесі Қағидаларда айқындалған тәртіппен (жаңа) тіркеу куәлігін шығару рәсімінен қайта өтеді.

96. Бұл ретте алдымен тіркеу куәлігінің иесі қолданыстағы тіркеу куәлігін кері қайтарып алуға өтініш, содан кейін жаңасын шығаруға өтініш береді.

§7. Тіркеу куәліктерін кері қайтарып алу

97. Тіркеу куәлігін кері қайтарып алу тіркеу куәлігінің иесі немесе КО ресімдеген өтініш бойынша жүзеге асырылады.

98. Тіркеу куәлігін қайтарып алуға өтініштер негіздер анықталған сәттен бастап дереу беріледі.

99. Тіркеу куәлігін кері қайтарып алу үшін тіркеу куәлігінің иесі-жеке тұлға тіркеу орталығы арқылы реттеушінің құқықтық актісіне сәйкес нысан бойынша тіркеу куәлігін кері қайтарып алуға өтініш береді.

100.КО тіркеу куәлігін келесі жағдайларда қайтарып алады:

1) тіркеу куәлігі иесінің талабы бойынша;

2) тіркеу орталығы анық емес мәліметтерді ұсыну фактісін не тіркеу куәлігін алған кезде құжаттардың толық емес топтамасын анықтаған кезде;

3) тіркеу куәлігі иесінің қайтыс болуы;

4) тіркеу куәлігі иесінің тегі, аты немесе әкесінің аты (егер ол жеке басты куәландыратын құжатта көрсетілсе) өзгертілсе;

5) соттың заңды күшіне енген шешімі бойынша.

Куәландырушы орталық осы тармақтың 1) тармақшасын қоспағанда, осы тармақта көрсетілген жағдайлардың бірі басталған кезде өтініш берушіден өтінішсіз тіркеу куәлігін кері қайтарып алуды жүргізеді.

101. Тіркеу куәлігі иесінің талабы бойынша тіркеу куәлігін кері қайтарып алу бір жұмыс күні ішінде жүзеге асырылады.

102. ҚР заңнамасында айқындалған тіркеу куәлігін кері қайтарып алу үшін негіздер тізбесі өзгерген жағдайда ҚР қолданыстағы заңнамасының талаптары қолданылады. Осы қағидалар белгіленген тәртіппен ҚР заңнамасына сәйкес келтірілуге тиіс.

103. Тіркеу орталығы тіркеу куәлігінің иесінен ресімделген тіркеу куәлігін қайтарып алуға өтініштерді өңдейді.

104. Тіркеу куәлігін қайтарып алмас бұрын өтініш беруші тіркеу орталығында сәйкестендіруден өтеді.

105. Тіркеу куәлігін кері қайтарып алу рәсімі реттеушінің құқықтық актісіне және Қағидалардың осы тарауына сәйкес жүзеге асырылады.

106.Сенім білдірілген тараптар өз іс-әрекеттеріне сүйенетін барлық тіркеу куәліктерінің мәртебесін тексереді.

107.110. Сенім білдіруші тараптардың тіркеу куәліктерінің мәртебесін тексерудің үздіксіз мүмкіндігін қамтамасыз ету үшін КО:

1) Қағиданың 3 тарауына сәйкес хатта жаңартылатын ҚТКТ жариялайды;

2) OCSP хаттама қызметінің жұмыс істеуін қамтамасыз етеді (OCSP – УО шығарған тіркеу куәліктерінің мәртебесі туралы ақпарат алуға арналған сервис (RFC 2560 "X. 509 Internet Public key Infrastructure ұсынымдарына сәйкес. Online Certificate Status Protocol-OCSP", X. 509 ашық кілттер интернет инфрақұрылымы сертификаттарының мәртебесінің онлайн хаттамасы)).

108.111. КО тіркеу куәлігінің қолданылуын уақытша тоқтата тұру немесе қайта бастау бойынша қызметтерді ұсынбайды.

109.КО тіркеу куәлігі иесінің жабық кілтін сақтау бойынша қызметтерді ұсынбайды.

110.Тіркеу куәліктерін пайдаланушылар (сенім білдіруші тараптар) өз іс-әрекеттеріне сүйенетін барлық тіркеу куәліктерінің мәртебесін тексеруге міндеттенеді.

111.Егер тіркеу куәлігін пайдаланушы (сенім білдіруші тарап) тіркеу куәлігінің мәртебесін тексеру үшін OCSP хаттама қызметіне онлайн өтінішті пайдаланбаса, онда ол бұл үшін КО қоймасында жарияланған өзекті ҚТКТ-ны пайдалануы тиіс.

112.КО-ның өзекті ҚТКТ-ны КО-ға қызмет көрсету деңгейі туралы келісімнің талаптарына сәйкес жоспарлы профилактикалық жұмыстардың уақытын қоспағанда, Банктің корпоративтік интернет-ресурсында тәулік бойы және үздіксіз қолжетімді.

113.Мерзімі өткен тіркеу куәліктерін ҚТКТ-тан алып тастау сертификаттау орталығының тиісті баптауымен айқындалған интервалдан кем емес жүзеге асырылады.

114.Жаңа ҚТКТ Банктің корпоративтік интернет-ресурсында қалыптастырылады және жарияланады: кез келген АКИ қатысушысының тіркеу куәлігін кері қайтарып алу фактісі бойынша не Сертификаттау орталығының тиісті баптауымен айқындалған кесте бойынша (егер белгіленген мерзім ішінде бірде-бір тіркеу куәлігі кері қайтарып алынбаса).

115. Жаңадан құрылған ҚТКТ автоматты түрде КО қоймасында қалыптастыру фактісі бойынша дереу сақталады.

116. Тіркеу куәліктерінің иесінің КО да қызмет көрсетуді тоқтату мүмкіндігі бар:

1) қызмет көрсетуді көздейтін қолданыстағы шартты (барлығын) бұзу;

2) қолданыстағы тіркеу куәлігін оның қолданылу мерзімі аяқталғанға дейін кері қайтарып алу.

117. Иеленушінің тіркеу куәлігінің қолданылу мерзімі өткен жағдайда КО-да иеленушіге қызмет көрсету автоматты түрде тоқтатылады.

118.КО жабық кілттері бұзылған жағдайда, КО әкімшісі бұл туралы сертификаттау орталығы мен тіркеу орталығының сервистерін пайдаланатын Банк АЖ бизнес иелеріне хабарлайды.

6-тарау. Куәландырушы орталықты бақылау түрлері (физикалық, операциялық, басқарушы)

§1. Физикалық бақылау

119. АКИ қатысушыларының сұраныстарын өңдейтін сертификаттау орталығы Банктің мамандандырылған деректер орталықтарында орналасқан.

120. КО-ның барлық үй-жайлары смарт-карталар бойынша сәйкестендірумен қол жеткізуді бақылау және басқару жүйесімен, келесілерге сәйкес электромеханикалық үлгідегі қол жеткізуді бақылау жүйесінің атқарушы құрылғыларымен жабдықталған:

1) өткізу және объектішілік режимді ұйымдастыру рәсімін регламенттейтін ІҚ-ға;

2) кіруді бақылау және басқару жүйелерін монтаждау және орналастыру тәртібін реттейтін ІҚ;

3) күзет теледидары жүйелерін монтаждау және орналастыру тәртібін регламенттейтін ІҚ.

121.Сертификаттау орталығының техникалық құралдары үздіксіз қоректендіру жабдықтарын пайдалана отырып, жалпы қалалық электрмен жабдықтау желісіне қосылған.

Сертификаттау орталығында пайдаланылатын электр желілері мен электр жабдықтары серверлік үй-жайларды техникалық жарақтандыру тәртібін регламенттейтін ІҚ-ға сәйкес қолданыстағы қауіпсіздік техникасы қағидаларының талаптарына жауап береді. КО үй-жайлары ҚР заңнамасында белгіленген СНжҚ санитариялық-гигиеналық нормаларына сәйкес температуралық-ылғалдылық режимінің, ауаны желдету мен тазартудың белгіленген параметрлерінің сақталуын қамтамасыз ететін желдету және ауаны баптау құралдарымен жабдықталған.

122.Сертификаттау орталығының жабдығын ылғалдан қорғау оны серверлік үй-жайларды техникалық жарақтандыру тәртібін регламенттейтін ІҚ сәйкес арнайы серверлік шкафтарда орналастырумен қамтамасыз етіледі.

123. Сертификаттау орталығы орналасқан үй-жай ҚР заңнамасында белгіленген талаптарға сәйкес өрт сөндіру құралдарымен жабдықталған.

124. Сертификаттау орталығының құжаттық мұрағаты ҚР қолданыстағы заңнамасына сәйкес сақталады.

125. Мұрағаттық сақтауға жатпайтын жоюға бөлінген құжаттарды және оларды жоюды құжаттаманы қамтамасыз ететін КО қызметкерлері жүзеге асырады. Ауыстырылатын ақпарат тасығыштар кәдеге жарату алдында физикалық түрде жойылады.

126. Тіркеу орталығының қызметі тек физикалық қорғалған объектілерде, рұқсат етілмеген қол жеткізу, пайдалану немесе құпия ақпаратты ашу әрекеттері қиын және тіркелген жағдайларда ғана келесілерге сәйкес жүзеге асырылады:

1) кіруді бақылау және басқару жүйелерін монтаждау және орналастыру тәртібін регламенттейтін ІҚ;

2) күзет теледидары жүйелерін монтаждау және орналастыру тәртібін регламенттейтін ІҚ;

3) өткізу және объектішілік режимді ұйымдастыру рәсімін регламенттейтін ІҚ;

4) серверлік үй-жайларды техникалық жарақтандыру тәртібін регламенттейтін ІҚ.

127. Сертификаттау орталығы төтенше жағдай кезінде резервтеу және жұмыс істеуін қалпына келтіру мақсатында әртүрлі объектілерде орналасқан 2 (екі) деректерді өңдеу орталықтарымен (негізгі және резервтік) қамтамасыз етілген.

128. Деректерді өңдеудің негізгі және резервтік орталығының физикалық қолжетімділігі өткізу және объектішілік режимді ұйымдастыру рәсімін регламенттейтін ІҚ-ға сәйкес бірдей қауіпсіздік шараларымен ұйымдастырылады және бақыланады.

129.Өңдеу орталықтарының серверлік үй жайлары жүйелермен жабдықталған:

1) кіруді бақылау және басқару;

2) күзет дабылы;

3) бейнебақылау;

4) кепілдендірілген электрмен жабдықтау;

5) электрлік жерге тұйықтау;

6) микроклиматты қамтамасыз ету;

7) өрт дабылы;

8) газды автоматты өрт сөндіру.

130. Банкте өткізу және объектішілік режим шараларын іске асыратын бөлімшелер сертификаттау орталығынан тәуелсіз болып табылады. Банкте өткізу және объектішілік режим шараларын іске асыратын процестерді бақылауды банкте өткізу және объектішілік режимдерді ұйымдастыру рәсімін регламенттейтін ІҚ-ға сәйкес қауіпсіздік бөлімшесі және Банктің ішкі құжатына сәйкес тәуелсіз бағалау арқылы ішкі аудит қызметі қамтамасыз етеді.

§2. Операциялық бақылау

131. КО-ның деректерді өңдеу орталықтары жабдықты қайта жүктеуді және жиынтықтауыштарды ауыстыруды қамтитын 24/7/365 онлайн режимінде тәулік бойы техникалық қолдаумен қамтамасыз етіледі.

132.Мүдделі Банктің АЖ тарапынан сертификаттау орталығының қызмет көрсету деңгейіне қойылатын талаптар:

1) сервистердің қолжетімділігі-24/7/365 режимінде 99,5%, яғни жоспарлы жұмыстарды есепке алмағанда, жылына 1 (бір) тәуліктен 19 (он тоғыз) сағаттан және 50 (елу) минуттан аспайды;

2) әр түрдегі сұраныстарды өңдеу жылдамдығы минутына 8 (сегіз) сұраныстан төмен емес;

3) операциялық қол жетімділікте кемінде 4 000 000 (төрт миллион) тіркеу куәлігіне қызмет көрсету.

133. Қызмет көрсету деңгейі туралы келісім бойынша жабдықтар мен байланыс арналарының істен шығуы себебінен деректерді өңдеу орталықтарындағы жабдықтың рұқсат етілген тоқтап қалу уақыты қызмет көрсетушілердің бақылауынан тыс жағдайларды немесе форс-мажорлық мән-жайлар жөніндегі жоспарлы жұмыстарды қоспағанда, жылына 18 (он сегіз) сағаттан аспайды (99.8% (тоқсан тоғыз мың сегіз онынші пайыз)).

134. Деректер орталықтары қызметтерін жеткізушінің реакция уақыты-тіркеу орталығы өтінімді ресімдеген сәттен бастап 1 (бір) сағаттан аспайды.

135. КО жұмыс процедураларының барлық жиынтығынан арнайы ұйымдастырушылық шаралармен аппараттық криптографиялық модульдерді (Hardware security Module, HSM) баптау және қызмет көрсету процедуралары және олардың негізгі материалдары КО бағдарламалық жасақтамасын орнатуды және конфигурациялауды реттейтін ІҚ-ға сәйкес бөлінеді.

136.HSM құрылғыларына кілттерді енгізген сәттен бастап HSM және кілттерге физикалық қол жеткізу үшін Банктің кемінде 2 (екі) уәкілетті қызметкерінің қатысуы қажет.

137. HSM (КО әкімшісі, КО жүйелік әкімшісі) жұмысын жүзеге асыратын қызметкерлер кілттермен физикалық және керісінше жұмыс істемейді.

§3. Басқарушылық бақылау

138. Сертификаттау орталығына қызмет көрсету жөніндегі қызметкерлерді қызметке тағайындау алдында ізденушілер ҚР Еңбек кодексінде айқындалған құжаттарды ұсынады және Банктің персоналды іріктеу жөніндегі процестерін регламенттейтін ІҚ сәйкес скринингтен өтеді.

139.Сертификаттау орталығына қызмет көрсетуге байланысты КО қызметкерлері мен басшылары біліктілік талаптарына сәйкестігі үшін 3 (үш) жылда кемінде 1 (бір) рет оқытудан немесе сертификаттаудан өтеді.

140. Лауазымдарға қойылатын біліктілік талаптарын қоспағанда, қызмет бойынша сертификаттау орталығына қызмет көрсетуге байланысты КО қызметкерлерінің орын ауыстыру жиілігі мен реттілігіне шектеулер қойылмайды.

141.Қызметтік ақпаратқа рұқсатсыз қол жеткізгені және ақпараттық қауіпсіздік талаптарын өзге де бұзғаны үшін сертификаттау орталығына қызмет көрсететін КО қызметкерлерінің жауапкершілігі еңбек шартында және лауазымдық нұсқаулықтарда көзделген.

142.Ақпараттық қауіпсіздік талаптарын бұзу фактісі бойынша тәртіптік жазалар банк қызметкерлеріне тәртіптік жазаларды қолдануды регламенттейтін ІҚ-ға сәйкес айқындалады және бұйрықтармен шығарылады.

143. Лауазымдық міндеттерін құзыретті атқару үшін сертификаттау орталығына қызмет көрсететін әрбір КО қызметкеріне ҚР заңнамасының құқықтық актілерінің және Банктің ІҚ мәтіндеріне қолжетімділік қамтамасыз етіледі.

§4. Бақылау хаттамалау рәсімдері

144.Бақылау хаттамасының жазба құрылымы мыналарды қамтиды:

1) жазу күні мен уақыты;

2) жазбаның реттік нөмірі;

3) оқиғаға бастамашылық жасаған, хаттамалауға жататын субъектінің сәйкестігі;

4) оқиға түрі;

5) жазба көзі.

145.Оқиға хаттамалары күн сайын хэшке айналады және хэш деректері блокчейн оқиғалар тізбегінде сақталады. Бұл үшін қолданылатын блокчейн интернетте қол жетімді.

146. КО-да оқиғалардың мынадай түрлері міндетті түрде хаттамалауға жатады:

1)КО кілттерінің өмірлік циклі (кілттерді жасау және жою, резервтік көшірмелерді жасау, сақтау, қалпына келтіру және жою);

2)тіркеу куәліктерінің өмірлік циклі (тіркеу куәліктерін шығаруға және олардың мәртебесін өзгертуге сұрау салу алу, тіркеу куәліктерін жасау және олардың мәртебесін өзгерту, ҚТКТ генерациялау және шығару);

3) HSM аппараттық криптографиялық модульдерінің өмірлік циклі (алу, пайдалануға беру, пайдалану-техникалық құжаттамамен айқындалған штаттық рәсімдер, сервистік қызмет көрсету, жөндеу, пайдаланудан шығару, жою);

4) шығаруға және тіркеуді Кери қайтарып алуға арналған өтініштердің өмірлік циклі (сәйкестендіру және аутентификация деректері, өңдеу күні мен уақыты);

5) банктің ақпараттық қауіпсіздік саясатына сәйкес хаттамалауға жататын өзге де оқиғалар (КО АЖ компоненттерін әкімшілендіру сессиялары, ақпараттық қауіпсіздік инциденттері және басқалар).

147.Кілттер мен оларды іске қосу деректері бақылау хаттамаларына жазылуға жатпайды.

148.КО бақылау хаттамаларын сертификаттау орталығы үздіксіз жүргізеді, Қағидалардың 6-тарауына сәйкес тәуліктік резервтік көшірмелеуге, ай сайынғы мұрағаттауға және мұрағатқа тапсыруға жатады, онда тіркеу куәлігінің қолданылу мерзімі өткен күннен бастап 1 (бір) жыл бойы сақталады.

149. Тіркеу куәліктері иелерінің және КО контрагенттерінің құжаттары (өтініштері және өзге де растайтын құжаттар) іс жүргізу мәселелері бойынша процестерді реттейтін Банктің ІҚ-ға сәйкес тіркеледі, жүйеленеді және сақталады.

§5. Куәландырушы орталықтың кілттерін ауыстыру

150.КО кілттерін ауыстыру олардың қолданылу мерзімі аяқталғанға дейін алдын ала жүзеге асырылады.

151.КО-ның жаңа кілттері мерзімі біткен кілттерді ауыстыруға немесе жаңа сервистерді пайдалануға беруді қамтамасыз ету мақсатында қолданыстағыларға қосымша жасалады.

152.Тіркеу куәліктерін пайдаланушылардың (сенім білдіруші тараптардың) КО-ның жаңа кілттерін пайдалануға өтуінің тегістігі КО-ның жаңа кілттерін тіркеу куәліктерін шығару және жоспарлы ауысуға жататын КО кілттерімен иелердің жаңа тіркеу куәліктеріне қол қоюды тоқтату есебінен қамтамасыз етіледі. Бұл ретте, КО өзінің көмегімен қол қойылған соңғы тіркеу куәлігінің қолданылу мерзімі аяқталған сәтке дейін қолданылу мерзімі аяқталатын кілтпен ҚТКТ-ға қол қоюды жалғастырады.

153.Алдын ала, КО уәкілетті тұлғасының жабық кілтінің қолданылу мерзімі аяқталғанға дейін КО әкімшісі жаңа жабық кілтті және КО уәкілетті тұлғасының тіркеу куәлігін қалыптастырады және оны қойманың тиісті бөліміне жариялайды. Жабық кілттің әрекеті аяқталғаннан кейін жабық кілті және оның көшірмелері бар негізгі ақпарат тасығыштар акт бойынша жойылады. Тіркеу куәліктерінің барлық иелері мен пайдаланушылары КО ның жаңа тіркеу куәлігін алуға және оны қолданыстағы КО тіркеу куәлігін жоймай тіркеу куәліктерінің анықтамалықтарына қосуға міндетті.

§6. Төтенше жағдайлар немесе әшкерелеу жағдайында жұмыс істеуді қалпына келтіру

154. КО сервистерінің жұмыс істеуін тоқтатуға әкеп соғатын төтенше жағдайлар болған жағдайда, Куәландырушы орталық қызметкерлерінің штаттан тыс, дағдарыстық жағдайлардағы іс-әрекеттері жөніндегі нұсқаулыққа (бұдан әрі - Штаттан тыс, дағдарыстық жағдайлардағы нұсқаулық), куәландырушы орталықтың ақпараттық жүйелерінің деректерін резервтік көшіру, мұрағаттау және қалпына келтіру жөніндегі нұсқаулыққа (бұдан әрі - Резервтік көшіру жөніндегі нұсқаулық) және Ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидаларға (бұдан әрі – Активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидалар) сәйкес іс-әрекеттер орындалады.

155. Штаттан тыс, дағдарыстық жағдайлардағы нұсқаулықтар, Резервтік көшіру жөніндегі нұсқаулықтар және Активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидалар:

1) қалпына келтіру үшін жұмыс деректер орталығына ауысу;

2) негізгі немесе резервтік деректер орталығының базасында қалпына келтіру алаңын таңдау және резервтік немесе мұрағаттық көшірмеден жұмыс жазбаларын қалпына келтіру.

156. Резервтік деректер орталығы қосалқы жабдықтармен қамтамасыз етілген. КО жұмыс жазбаларының резервтік және мұрағаттық көшірмелерін жасау және сақтау штаттан тыс, дағдарыстық жағдайлардағы нұсқаулықтарда, резервтік көшіру жөніндегі нұсқаулықтарда және активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидаларда регламенттелген.

157. Есептеу, бағдарламалық ресурстар және/немесе ақпараттық жүйенің деректері бүлінген жағдайда КО Штаттан тыс, дағдарыстық жағдайлардағы нұсқаулыққа және Активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидаларға сәйкес өңделеді.

158.КО тіркеу куәлігін қайтарып алу туралы шешім қабылдаған жағдайда КО мынадай рәсімдерді орындайды:

1) кері қайтарып алу туралы ақпарат қағидаларға сәйкес ҚТКТ-да жарияланады;

2) Штаттан тыс, дағдарыстық жағдайлардағы нұсқаулыққа және активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидаларға сәйкес КО тіркеу куәлігін қайтарып алу туралы сенім білдіруші тараптарды қосымша хабардар ету үшін өзге де орынды шаралар қабылданады;

3) КО қызметін тоқтату жағдайларын қоспағанда, қағидаларға сәйкес жаңа кілттер жасалады.

159.Штаттан тыс, дағдарыстық жағдайларда нұсқаулықтың, резервтік көшіру жөніндегі нұсқаулықтың және Активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидалардың өзектілігі сертификаттау орталығында өзгерістер енгізілуіне қарай немесе сертификаттау орталығын негізгі және резервтік деректер орталықтары арасында ауыстыру нәтижелері бойынша, бірақ жылына кемінде 1 (бір) рет тексеріледі.

160.Деректер орталықтарындағы КО жабдығы бірнеше арналарды пайдалана отырып желіге резервтелген қосылумен қамтамасыз етіледі.

161. КО деректер базасындағы барлық өзгерістер деректер орталықтары арасында үнемі қайталанады.

162. КО ның жабық кілттерінің бұзылуына негізделген күдік сыни деңгейдегі ақпараттық қауіпсіздік оқиғасы ретінде қарастырылады.

163. КО деректерінің резервтік жабдығының, резервтік және мұрағаттық көшірмелерінің дайындығын тексеру резервтік көшіру жөніндегі нұсқаулықты, штаттан тыс, дағдарыстық жағдайлардағы нұсқаулықтарды және активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидаларды пайдалана отырып, негізгі және резервтік деректерді өңдеу орталықтары арасында сертификаттау орталығының жұмысын жылына кемінде 1 (бір) рет ауыстыру жолымен жүзеге асырылады.

164. КО жұмысын тоқтату туралы шешім қабылданған жағдайда тіркеу куәліктерінің иелері мен пайдаланушыларын (иелері мен сенім білдіруші тараптарды) қоса алғанда, Банктің контрагенттерін хабардар ету, КО жазбаларын беру және мұрағаттық сақтау "Электрондық құжат және электрондық цифрлық қолтаңба туралы"ҚР Заңына сәйкес ұйымдастырылады.

§7. Мұрағатты жүргізу

165.КО мыналардың мұрағатын жүргізеді:

1) кері қайтарып алынған тіркеу куәліктерін және қолданылу мерзімі өткен тіркеу куәліктерін қоса алғанда, шығарылған тіркеу куәліктері;

2) тіркеу куәліктерінің шығарылуы және кері қайтарып алынуы туралы өтініштерді қоса алғанда, олардың өмірлік циклі туралы ақпарат және ҚТКТ;

3) ақпараттық жүйенің бақылау хаттамалары.

166.Мұрағаттық ақпарат тасығыштарды сақтау, мұрағаттық ақпарат тасығыштарды таңбалау, мұрағат деректерін рұқсатсыз қараудан, өзгертуден және жоюдан қорғау резервтік көшіру жүйесінің магниттік таспаларын және серверлік жабдық пен деректерді сақтау жүйелерінің қатты дискілерін пайдалану жөніндегі нұсқаулыққа сәйкес жүзеге асырылады.

167.КО құпия деректер тасымалдағыштарын кәдеге жарату магниттік таспаларды резервтік көшіру жүйесін және қатты дискілерді серверлік жабдықтарды және деректерді сақтау жүйелерін пайдалану жөніндегі нұсқаулыққа сәйкес жүзеге асырылады.

168.КО қызметін тоқтату туралы шешім қабылданған жағдайда мұрағат деректері ҚР заңнамасында белгіленген мерзім ішінде сақталуға тиіс.

169. Мұрағатқа қол жеткізу тек сертификаттау орталығына қызмет көрсететін КО қызметкерлеріне ғана беріледі.

170.Сертификаттау орталығының мұрағатын сыртқы резервтеу көзделмейді.

7-тарау. Техникалық қауіпсіздікті бақылау

§1. Кілттерді құру және орнату

171.Кілттерді генерациялаудың әрбір фактісі бойынша сертификаттау орталығы хаттама жасайды, оған рәсімге қатысқан адамдар қол қояды және қол қояды. Хаттамалар іс жүргізу мәселелерін реттейтін Банктің ІҚ сәйкес сақталады.

172.Қызметкерлердің немесе тіркеу орталығының тіркеу куәліктері иелерінің жабық кілттеріне қол жеткізуі тек негізгі ақпараттың қорғалған тасымалдағыштарын пайдалану арқылы техникалық тұрғыдан алынып тасталады.

173.КО және оның иелерінің ашық кілттерінің тұтастығы мен тиесілігі оларды генерациялаудан бастап тіркеу куәліктерін шығаруға дейінгі кезеңде ЭЦҚ тетігімен қорғалады. Ашық кілттер иеленушілерден КО- ға тек PKCS#10 форматындағы электрондық құжаттар нысанында беріледі.

174.КО ның ашық кілттері сенім білдірілген тараптарға тіркеу куәліктері нысанында беріледі.

175.Тіркеу куәліктерінің иелері КО-ның ашық кілттерін жеке немесе тізбектің бір бөлігі ретінде өздерінің тіркеу куәліктеріне сұрата алады.

176.КО-ның ашық кілттері (тіркеу куәліктерінің құрамында) Банктің корпоративтік интернет-ресурсынан жүктеу үшін де қолжетімді.

177.КО МЕМСТ 34.310-2004 халықаралық стандартына (ЭЦҚ)сәйкес пайдалануға арналған кілттерді береді:

Жабық кілттің ұзындығы - 256 екілік разряд.

Ашық кілттің ұзындығы - 512 екілік разряд.

178.ЭЦҚ жабық кілттерін бұлтты ЭЦҚ- да КО жасайды.

179.Бұлтты ЭЦҚ-ның жабық кілттері HSM Модулінің ішінде қатаң түрде жасалады. ЭЦҚ-ның жабық кілті HSM-ден ашық түрде алынбайды. ЭЦҚ Модулінің GSM талаптары:

1) ҚР СТ 1073-2007 "ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар";

2) корпусты ашу фактісін анықтау және HSM үшін қажетті негізгі ақпаратты кейіннен жою үшін датчиктерді пайдаланатын периметрдің физикалық қорғанысымен (корпусты ашудан қорғау) жобаланған;

3) ҚР қолданыстағы заңнамасының талаптарына сәйкес ақпарат пен техникалық құралдардың қорғалуын бағалау әдістемесіне және қорғау тиімділігінің нормаларына сәйкес келеді.

Негізгі ақпарат тасығыштармен барлық іс-әрекеттер оларды пайдалану жөніндегі нұсқаулықтарға және қауіпсіздік талаптарына сәйкес қатаң түрде жүзеге асырылуға тиіс.

§2. Жабық кілттерді қорғау және инженерлік бақылау криптографиялық модульдер

180.Сертификаттау орталығында иелердің жабық кілттері оны жария ету, өзгерту немесе рұқсатсыз пайдалану мүмкіндігін болдырмайтын негізгі ақпараттың қорғалған тасымалдаушысында тікелей жасалады.

181.HSM ішінде іске қосылған КО кілттерімен операцияларды орындау үшін КО-ның кемінде 2 (екі) уәкілетті қызметкерінің қатысуы талап етіледі.

182.Жоғарыда көрсетілген HSM, олардың құрамдас бөліктері мен бөлшектері банктен шығуға немесе кез келген басқа сапада қайта пайдалануға жатпайды.

183.КО жабық кілттерін генерациялауды сертификаттау орталығы тікелей осы кілттер бірінші рет қолданылатын аппараттық криптографиялық модульде (HSM) жасайды. Жаңадан жасалған жабық кілттерді қосымша белсендіру қажет емес.

184.Құрылғаннан кейін КО-ның жабық кілттері депозитке жатпайды. Сонымен қатар, төтенше оқиғадан немесе жұмыстағы өзге де іркілістен кейін АЖ жұмыс істеуін қалпына келтіру мүмкіндігін қамтамасыз ету мақсатында сертификаттау орталығы әрбір жаңа жабық кілт жасалғаннан кейін тікелей ағымдағы сәтте пайдаланылатын барлық жабық х кілттердің резервтік көшірмесін жасайды және сақтайды.

185.Сақтық көшірмені жасау барысында жабық кілттерді КО жүйелік әкімшісі аппараттық криптографиялық модульден (HSM) шифрланған түрде шифрлайды және түсіреді, қалпына келтіру барысында-кері тәртіпте, сақтық көшірме HSM-ге шифрланған түрде жүктеледі және жабық кілттер құрылғының ішінде шифрланады.

186.Аппараттық криптографиялық модульден (HSM) КО жабық кілттерінің сақтық көшірмесін түсіру кезінде n бөлікке бөлінетін құпия (белсендіру деректері) жасалады. Кілттерді резервтік көшірмеден қалпына келтіргеннен кейін іске қосу үшін олардың сақтаушыларының қатысуымен құпияның m бөліктерін тарту жеткілікті. М-ден m параметрлерінің ағымдағы мәні HSM паспортында тіркелген (осы Қағидалар шығарылған кезде n = 3 және m = 2).

187.Құпия бөліктері мен КО жабық кілттерінің резервтік көшірмелерін сақтаушылардың лауазымдық құрамы КО кілттерін генерациялау хаттамасында тіркеледі.

188.Сертификаттау орталығының үздіксіз жұмыс істеуін қамтамасыз ету мақсатында аппараттық криптографиялық модульдердегі (HSM) жабық кілттер олар жасалғаннан немесе резервтік көшірмеден қалпына келтірілгеннен кейін жойылғанға (жойылғанға)дейін белсенді болып қалады.

189.Ауыстыру немесе қолданылу мерзімінің аяқталуы салдарынан өзектілігін жоғалтқан КО жабық кілттерін КО жүйелік әкімшісі ақпаратты криптографиялық қорғаудың сертификатталған құралдарының пайдалану-техникалық құжаттамасына сәйкес аппараттық криптографиялық модульдердің (HSM) штаттық функцияларымен жояды.

190.Сақтау кезеңінде КО жабық кілттерінің резервтік көшірмесі криптографиялық және ұйымдастырушылық шаралардың жария етілуінен, бұрмалануынан және ауыстырылуынан қорғалған.

191.Аппараттық криптографиялық модульден (модульге) (- m) (HSM) түсіру (жүктеу) кезінде КО жабық кілттерінің резервтік көшірмесін шифрлауды КО жүйелік әкімшісі іске қосу деректерін бөліктерге бөлінген құпия нысанында жасай отырып (пайдалана отырып) жүзеге асырады, олардың әрқайсысы жеке жауапты тұлғаға (құпияның бір бөлігін сақтаушыға) бекітіледі, қорғалған ақпарат тасығышқа жазылады және жеке парольмен қорғалады.

192.Ауыстыру немесе қолданылу мерзімінің аяқталуы салдарынан өзектілігін жоғалтқан КО жабық кілттерінің резервтік көшірмелері мұрағаттық сақтауға жатпайды және Ко жүйелік әкімшісі Банктің ІҚ сәйкес Электрондық ақпаратты және ақаулы электрондық тасымалдағыштарды жою процестерін регламенттейтін жойылады.

193.Пайдалану мерзімінің өтуі салдарынан пайдаланудан шығарылған немесе сынғаннан кейін жөндеуге келмейтін Сертификаттау орталығының өнімді ортасының жабық кілттері болған аппараттық криптографиялық модульдер (HSM), HSM тестілік сынақтарын қоспағанда, банктен шығуға немесе жекелеген тораптар мен бөлшектерге бөлуді қоса алғанда, кез келген өзге де сапада қайта пайдалануға жатпайды. Баланстан шығарылғаннан кейін жоғарыда аталған HSM Электрондық ақпаратты және ақаулы электрондық тасымалдағыштарды жою процестерін регламенттейтін ІҚ-ға сәйкес жойылуға жатады.

§3. Кілттерді басқарудың басқа аспектілері

194.Ашық кілті КО шығарған тіркеу куәлігімен куәландырылған кез келген кілттер жұбын пайдалану кезеңі Тіркеу куәлігінің қолданылу мерзіміне сәйкес келеді, тек ақпаратты ашу немесе ЭЦҚ тексеру мақсатында тиісті кілттер тіркеу куәлігінің қолданылу мерзімі өткеннен кейін де пайдаланылуы мүмкін.

195.КО тіркеу куәлігінің қолданылу мерзімі кемінде 20 (жиырма) жылды құрайды және ол шығарылған күнінен және уақытынан бастап есептеледі.

196.Тіркеу орталығы арқылы келіп түскен иелердің тіркеу куәліктерінің қолданылу мерзімі 1 (бір) жылды құрайды және Қағидалардың 3-тарауының 3-параграфына сәйкес Банктің АЖ мүдделі нормативтік-техникалық құжаттамасында белгіленеді.

197.КО шығарған тіркеу куәліктерінің болуын талап ететін АЖ-да үздіксіз жұмыс істеу үшін иелеріне Қағидаға сәйкес қолданылу мерзімі өтіп кеткен тіркеу куәлігін ауыстыру үшін жаңа тіркеу куәлігін шығаруды сұрату құқығы беріледі.

§4. Жабық кілтті белсендендіру деректері

198.Жабық кілтті пайдалану үшін КО иесі белсендіру деректерін пароль түрінде құруы және қолдануы керек.

199.Парольді орнату кезінде АКИ қатысушысы (тіркеу куәліктерінің иелерін қоспағанда) оны бірінші қосқаннан кейін бірден ауыстыруға (ауыстыруға) міндетті, бұл ретте пароль:

1) 8 (сегіз) таңбадан қысқа болмауы керек;

2) төменгі регистрде (кіші әріппен) кемінде 1 (бір) әріп болуы керек;

3) бас әріпте кемінде 1 (бір) әріп, 1 (бір) сан немесе 1 (бір) арнайы таңба болуы керек;

4) қайталанатын таңбалар болмауы тиіс.

200.Тіркеу орталығында пароль орнатқан кезде тіркеу куәлігінің иесі пароль енгізеді, оған мынадай талаптар белгіленген:

1) 4 (төрт) таңбадан қысқа болмауы керек;

2) тек цифрлық мәндерді қамтуы тиіс.

201.Кілтке кіру паролін жазуға тыйым салынады. Құпия сөз тек кілт иесіне белгілі болуы керек. Пайдаланылатын қауіпсіздік құралдарында парольді автоматты түрде сақтау функциясын пайдалануға тыйым салынады.

202.Тіркеу куәлігі иесінің жабық кілтін іске қосу үшін парольдер ақпараттық жүйелердегі пайдаланушыларды сәйкестендіру және аутентификациялау қағидаларының талаптарына сәйкес пайдаланылады.

203.КО-ның жабық кілттерін іске қосуға арналған құпияның бір бөлігінің әрбір сақтаушысы (АКИ қатысушысы) өзінің құпия сөзін құпия сақтайды және еңбек шартында және лауазымдық нұсқаулықта көзделген осы талапты бұзғаны үшін жауапты болады.

204.КО жабық кілттерін активтендіру деректері бар аппараттық таңбалауыштар активтендіру деректерінің өзектілігі жоғалған жағдайда қайта жазылады (нөлге теңестіріледі) және парольдердің резервтік көшірмелерін сақтау үшін көзделген тәртіппен сол мақсаттарда қайта пайдалану сәтіне дейін немесе кейіннен міндетті түрде жойыла отырып есептен шығарылғанға дейін сақталады. Құпияның бөліктерін сақтау үшін бұрын-соңды пайдаланылған қорғалған тасығыштар банктен шығуға, бөлшектеуге немесе өзге мақсаттарда қайта пайдалануға жатпайды.

§5. Есептеу ресурстарының қауіпсіздігін бақылау

205.OCSP қызметінің тіркеу куәліктеріне, ҚТКТ, жауаптарына (түбіртектеріне) қол қоюға арналған серверлер рұқсатсыз кіруден қорғалады.

206.Серверлердің операциялық жүйелеріне АЖ АҚ қамтамасыз ету рәсімін регламенттейтін ұсынылған қорғаныс пакеттері мен жаңартуларын, оның ішінде ІҚ-ға сәйкес антивирустық пакеттерді қолдану арқылы қорғаудың жоғары деңгейінде қолдау көрсетіледі.

207.Негізгі серверлерді басқаруға тек сертификаттау орталығына қызмет көрсетуге байланысты жұмысшыларға рұқсат етіледі, КО бағдарламалық жасақтамасының қалған пайдаланушылары жүйелік немесе технологиялық шоттарға қол жеткізе алмайды.

208.АКИ қатысушыларына қызмет көрсету үшін пайдаланылатын желі сегменттері Банктің қалған желісінен қисынды түрде бөлінген. Бұл бөлектеу пайдаланушылардың белгілі бір қолданбалы бағдарламалық процестер арқылы қол жеткізуден басқа КО деректеріне кез келген желілік қатынауын болдырмайды. Сертификаттау орталығының дерекқорларына тікелей қол жеткізу КО әкімшілерінің және КО жүйелік әкімшілерінің ең аз қажетті тобымен шектеледі.

209.КО желісінің сегменттерін сыртқы немесе ішкі араласудан қорғау, желілік белсенділіктің мазмұны мен көздерін шектеу үшін брандмауэрлер қолданылады.

210.Сертификаттау орталығының қызметінде стандарт талаптарына сәйкестігіне сертификатталған ақпаратты криптографиялық қорғау құралдары (АККҚ: HSM және бағдарламалық АККҚ) пайдаланылады.

211.Өзге (криптографиялық емес) компоненттердің және бағдарламалық қамтамасыз етудің ақпараттық қауіпсіздігін сертификаттау бойынша арнайы талаптар қойылмайды.

212.КО функциялары рұқсатсыз кіруден қорғау тәртібін регламенттейтін Банктің ІҚ сәйкес рұқсатсыз кіруден қорғалған сертификаттау орталығында орындалады.

213.КО модульдерінің (компонентінің) түсіндірме жазбамен өзара іс-қимыл схемасы Қағидаларға 1-қосымшада келтірілген.

§6. Желінің дамуы мен қауіпсіздігін басқаруды бақылау

214.КО өз қызметінде пайдаланатын барлық қолданбалы бағдарламалық қамтамасыз ету лицензияланған болып табылады, оған айрықша құқықтар банкке тиесілі емес.

215.КО өз қызметінде пайдаланатын қолданбалы бағдарламалық қамтамасыз етудің тиісінше жұмыс істеуін қамтамасыз ету жөніндегі міндеттемелерді өнім беруші шарт бойынша (сервистік ұйым)орындайды.

216.Сертификаттау орталығындағы кез келген өзгерістерді сынақтан өткізу мақсатында есептеу техникасының, ақпаратты криптографиялық қорғау құралдарының және

бағдарламалық жасақтаманы пайдалануға лицензиялардың қажетті минимумымен қамтамасыз етілген оның сынақ тізбегі бар және оны қолдайды.

217.Тіркеу куәліктері, ҚТКТ, OCSP түбіртек жауаптары (қызмет жауаптары), тіркеу куәліктерінің шығарылуы және мәртебесінің өзгеруі туралы ақпаратты қамтитын сертификаттау орталығының Бақылау хаттамалары оқиғалардың күні мен уақыты туралы ақпаратты қамтиды.

218.OCSP тіркеу куәліктерінде, ҚТКТ, түбіртектерде (қызметтің жауаптарында) қамтылған оқиғалардың күні мен уақыты туралы ақпарат КО ЭЦҚ-мен куәландырылады.

8 тарау. Тіркеу куәліктерінің профильдері, ҚТКТ және OCSP

§1. Тіркеу куәліктерінің профильдері

219.КО шығаратын тіркеу куәліктері 3 (V. 3)нұсқасы бойынша таңбаланған RFC 3280 ұсынымдарына сәйкес келеді.

220.Тіркеу куәліктеріндегі негізгі жолдар олардың мазмұнына қойылатын талаптармен бірге төменде көрсетілген кестеде келтірілген:

Атауы	Мазмұнға қойылатын талаптар
Version	V3
serialNumber	тіркеу куәлігінің бірегей сериялық нөмірі
signatureAlgorithm	subjectpublickeyinfo жолында көрсетілген кілт арналған криптографиялық алгоритмнің нысан идентификаторы
Issuer	C=KZ O=Jusan Bank JSC CN=Certification Authority
Validity	YYYYMMDDHHMMSSZ GMT (бастап жарамды) YYYYMMDDHHMMSSZ GMT (дейін жарамды)
Subject	C=KZ O= Jusan Bank JSC OU=Банктің логикалық немесе құрылымдық бірлігі, мысалы, Банктің ақпараттық жүйесі немесе ішкі жүйесі, Блок, Департамент немесе Банктің басқа бөлімшесі CN= иесінің коды (ТАӘ) UID= иесінің коды (ЖСН)
subjectPublicKeyInfo	ашық кілт
issuerSignatureAlgorithm	тіркеу куәлігіне қол қойылған криптографиялық алгоритмнің нысандық идентификаторы
signatureValue	электрондық цифрлық қолтаңба

221.КО шығаратын тіркеу куәліктерінде көрсетілген атаулар ITU-T X. 520 атау форматына сәйкес Қағидалардың талаптарына сәйкес келеді.

222.Тіркеу куәлігінде қолданылатын негізгі кеңейтімдер олардың синтаксисіне қойылатын талаптармен бірге төмендегі кестеде келтірілген:

Атауы	Сыншылдығы	Форматы
1	**2**	**3**
authorityKeyIdentifier	FALSE	OID 2.5.29.35 сәйкес
subjectKeyIdentifier	FALSE	OID 2.5.29.14 сәйкес
keyUsage	TRUE	OID 2.5.29.15 сәйкес
CertificatePolicies	FALSE	OID 2.5.29.32 сәйкес
basicConstraint	TRUE	OID 2.5.29.19 сәйкес
1	**2**	**3**
extendedKeyUsage	FALSE	OID 2.5.29.37 сәйкес
cRLDiistributionPoints	FALSE	OID 2.5.29.31 сәйкес
authorityInformationAccess	FALSE	OID 1.3.6.1.5.5.7.1.1 (RFC 2459) сәйкес

223.Тіркеу куәліктеріне қол қою үшін КО қолданатын криптографиялық алгоритм төменде көрсетілген кестеде келтірілген:

Атауы	Форматы
МЕМСТ 34.310-2004	{iso(1) member-body(2) kz(398) certification-authorities(3) basic-cryptography(10) algorithms(1) digital-signature(1) GOST-34.310-2004(1)}

224.ЭЦҚ тіркеу куәлігін қалыптастыру және пайдалану процесінде қолданылатын криптографиялық қайта құру алгоритмдеріне бастапқы деректері (негізгі талаптары) бар иелердің ЭЦҚ пайдалану және иелердің ЭЦҚ тіркеу куәлігін алу схемалары Қағидаларға 2-қосымшада келтірілген.

225.КО шығарған тіркеу куәліктері қолданылатын ақпараттық жүйелерге сәйкес тіркеу куәліктері саясатының Объектілік сәйкестендіргіштері Қағидаларға сәйкес белгіленеді. "CertificatePolicies" тіркеу куәліктерін кеңейту Қағидалардың осы тарауына сәйкес толтырылады.

§2. Кері қайтарып алынған тіркеу куәліктері тізімінің профильдері

226.КО шығаратын ҚТКТ 2 (V. 2) нұсқасы бойынша таңбаланған RFC 3280 ұсыныстарына сәйкес келеді.

227.ҚТКТ құрамындағы негізгі өрістер мен кеңейтімдер олардың мазмұнына қойылатын талаптармен бірге төмендегі кестеде келтірілген:

Атауы	Мазмұнға қойылатын талаптар
Version (optional)	V2
Issuer	C=KZ O=Jusan Bank JSC CN=Certification Authority
thisUpdate	YYYYMMDDHHMMSSZ GMT (бастап жарамды)
[nextUpdate (optional)	YYYYMMDDHHMMSSZ GMT (келесі жаңарту)]
signatureAlgorithm	қайтарылған тіркеу куәліктерінің тізіміне қол қойылған алгоритмнің нысандық идентификаторы
revokedCertificates	Келесі түрдегі жұптар тізбегі:
cRLNumber	1. certificateSerialNumber (тіркеу куәлігінің сериялық нөмірі);
authorityKeyIdentifier	2. Уақыт (кері қайтарып алу туралы өтінішті өңдеу уақыты
signatureValue	тіркеу куәлігі).

228.КО шығаратын ҚТКТ жазбаларында қолданылатын кеңейтімдер төмендегі кестеде келтірілген:

Атауы	Сыншылдығы
reasonCode	FALSE
certificateIssuer	FALSE

§3. OCSP қызметінің профилі

229.OCSP хаттамасы қазіргі уақытта көрсетілген тіркеу куәлігінің мәртебесін анықтау үшін сенім білдіруші тараптарға қажет.

230.КО шығарған тіркеу куәліктерінің мәртебесі туралы ақпарат алу үшін OCSP сервисін сертификаттау орталығы 1-нұсқа форматында ұсынады (RFC 2560 "X. 509 Internet Public key Infrastructure ұсынымдарына сәйкес. Online Certificate Status Protocol-OCSP", X. 509 ашық кілттер интернет инфрақұрылымы сертификаттарының мәртебесінің онлайн хаттамасы).

9-тарау. Қызметті тексеру

231.КО аккредиттеу "электрондық құжат және электрондық цифрлық қолтаңба туралы" ҚР заңнамасына сәйкес 3 (үш) жыл мерзімге тегін негізде жүзеге асырылады.

232.КО жұмысын қамтамасыз етуге қатысатын бөлімшелердің қызметі (КО әкімшісі, КО жүйелік әкімшісі, КО қауіпсіздік офицері, КО бастығы, КО кезекшісі) жоспарлы негізде аудит жүргізу тәртібін регламенттейтін Банктің ІҚ сәйкес ішкі аудитке жатады.

10-тарау. Басқа сұрақтар

§1. Тарифтер

233.Сертификаттау орталығы қызмет көрсетілетін ақпараттық жүйелердің пайдаланушыларына тарифтелмейтін және төленбейтін келесі қызметтерді ұсынады:

1) жеке тұлғалардың өтініштері бойынша тіркеуді қуалауын шығару;

2) тіркеу куәлігін кері қайтарып алу;

3) тіркеу куәліктері мен ҚТКТ-ні қоймаға орналастыру;

4) OCSP хаттамасы бойынша онлайн режимінде тіркеу куәліктерінің мәртебесі туралы ақпарат беру;

5)Tsp (Time stamp protocol - "уақыт белгілері"сервисі) хаттамасы бойынша деректерді онлайн режимінде нақты уақытқа байланыстыру.

§2. Қатысушылардың дербес деректерін қорғау

234.Тіркеу куәлігінің кез келген иесі КО-ға тіркеу куәлігін шығаруға өтініш бере отырып, ол өзі туралы ақпаратты жария түрде жариялауға келісім беретінін мойындайды.

235.Тіркеу куәлігін шығаруға өтініш субъектінің тіркеу куәліктері иелерінің дербес деректері және оларды қорғау мәселелері бойынша ҚР заңнамасына сәйкес оның дербес деректерін жинауға және өңдеуге келісімін білдіретін жазбаша құжат болып табылады.

236.О тіркеу куәліктерінің иелері туралы мәліметтерді қорғауды қамтамасыз етеді және оларды ҚР заңнамасында көзделген жағдайларда ашады.

237.Тараптардың келісіміне сәйкес құпия болып табылатын тіркеу куәліктерінің иелері туралы мәліметтер тіркеу куәліктерінің жалпыға қолжетімді тіркеліміне енгізілмейді.

§3. Зияткерлік меншік құқығы

238.Тіркеу куәліктерінің иелері тіркеу куәліктеріндегі атаулар мен сауда белгілеріне барлық құқықтарын сақтайды.

239.КО тіркеу куәліктерінің иелері мен пайдаланушыларына (меншік иесі мен сенім білдіруші тараптарға) деректердің толықтығы мен тұтастығы шарттарын сақтай отырып, тіркеу куәліктерін айрықша емес тегін негізде көшіруге және таратуға тыйым салмайды.

240.КО шығарған тіркеу куәлігіне сәйкес келетін жабық кілт осы тіркеу куәлігі иесінің меншігі болып табылады. Оған сәйкес келетін ашық кілт және тіркеу куәлігі банктің меншігі болып табылады.

§4. Кепілдіктер мен растамалар

241.Сертификаттау орталығы мыналарды:

1) ол шығарған тіркеу куәліктеріндегі деректердің Тіркеу орталығы Тіркеу куәгері шығарға сұрау салу құрамында берген мәліметтерге сәйкестігі және тіркеу куәліктерінде бұл мәліметтердің ниеті бойынша немесе КО қызметкерлерінің қате әрекеттері нәтижесінде кездейсоқ немесе қасақана бұрмалануының болмауын;

2) көрсетілетін қызметтердің (шығару, тіркеуді Кери қайтарып алу, ҚТКТ шығару, OCSP және TSP онлайн-сервистері) талаптарына сәйкестігі: электрондық құжат және электрондық цифрлық қолтаңба, саясат және ережелер мәселелері бойынша ҚР қолданыстағы заңнамасының талаптарын;

3) Банктің корпоративтік интернет ресурсында Саясат талаптары мен Қағидаларын жариялауды қамтамасыз етеді.

242.Тіркеу орталығы:

1) сертификаттау орталығына жіберілетін тіркеу куәлік шығарға арналған сауалдардағы деректердің сәйкестендіру рәсімдері барысында өтініш беруші ұсынған құжаттардағы мәліметтерге сәйкестігі және осы сауалдарда ниет бойынша енгізілген немесе АЖ бизнес-иелерінің қате әрекеттері нәтижесінде жіберілген қасақана немесе кездейсоқ бұрмалаулардың болмауын;

2) тіркеу орталығы орындайтын рәсімдердің (өтініш берушілердің шығаруға және тіркеуді керіқайтарып алуға өтініштерін тіркеу және өңдеу, өтініш берушілерді сәйкестендіру рәсімдері, иесіне тіркеу куәліктерін беру) және электрондық құжат және электрондық цифрлық қолтаңба, Саясат және Қағидалар мәселелері бойынша ҚР қолданыстағы заңнамасының талаптарына сәйкестігін қамтамасыз етеді.

243. Тіркеу куәлігінің әрбір иесі:

1) КО шығарған, иесі қабылдаған және пайдалану кезінде жарамды (мерзімі өтіп кетпеген немесе қайтарып алынбаған)тиісті тіркеу куәлігі бар өзінің жабық кілтін ғана пайдалану;

2) тіркеу орталығына тіркеу куәліктерін шығару үшін ұсынылатын өзі туралы мәліметтердің дұрыстығы;

3) тіркеу куәлігін қабылдағанға дейін тіркеу куәліктерінде қамтылған өзі туралы мәліметтердің дұрыстығын тексеру;

4) өзінің жабық кілтін қандай да бір тіркеу куәліктеріне, ҚТКТ-ға, ашық кілт куәліктерінің кез келген басқа форматына немесе оның мәртебесі туралы ақпаратқа қол қою мақсатында пайдаланбау.

244.Тіркеу куәлігінің әрбір иесі және әрбір пайдаланушысы (иесі және сенім білдіруші тарап) КО шығарған тіркеу куәліктерін пайдалану кезінде тіркеу куәлігі және оның иесі туралы объективті ақпараттың жеткілікті көлеміне сүйене отырып, тек негізделген шешімдер қабылдауды қамтамасыз етеді.

245. Сертификаттау орталығы электрондық құжат және ЭЦҚ мәселелері бойынша ҚР заңнамасында белгіленген және саясатпен декларацияланған жауаптылықтан басқа, тауарлық жарамдылығы мен сәйкестігі үшін жауапкершілікті қоса алғанда, банктік қызмет көрсету шарттарынан туындайтын тіркеу куәліктерінің иелері мен пайдаланушыларының (иесі мен сенім білдіруші тараптардың) алдында қосымша жауапкершілік көтермейді.

§5. Хабарламалар және қатысушылармен байланыс

246.АКИ қатысушылары: КО қызметкерлері, тіркеу куәліктерінің иелері мен пайдаланушылары (иелері мен сенім білдіруші тараптар) - бір-бірімен байланысу үшін өзара іс-қимыл тақырыбына, коммуникацияның маңыздылығы мен жеделдігіне сәйкес келетін кез келген орынды арналарды пайдаланады (корпоративтік интернет ресурс, электрондық пошта (e-mail), пошта байланысы, телефон байланысы, мобильді қосымша, интернет- банкинг, телебанкинг, телефон, және өзге де интернет-ресурстар), егер тараптар арасындағы келісімде өзгеше белгіленбесе.

§6. Дауларды шешу

247.Егер дау сотқа дейінгі тәртіппен шешілмесе, онда ол сот тәртібімен шешілуге тиіс.

248.Осы Қағидалардың мәні бойынша келіспеушіліктер нысанасы болып табылатын дауларды шешу үшін ҚР заңнамасы қолданылады.

249.Еңсерілмейтін күш (форс-мажор) мән-жайлары туындаған жағдайда АКИ қатысушылары: КО қызметкерлері, тіркеу куәліктерінің иелері мен пайдаланушылары (иелері мен сенім білдіруші Тараптар) - олардың арасында қолданылатын шарттардың тиісті ережелерін басшылыққа алады (бар болса).

11-тарау. Жауапкершілік

250.КО қызмет көрсететін АКИ қатысушыларының жауапкершілігі ҚР заңнамасымен белгіленген.

251.Сертификаттау орталығы мен тіркеу орталығына (КО әкімшісі, КО жүйелік әкімшісі, КО қауіпсіздік офицері, КО бастығы, КО кезекшісі) қызмет көрсетуге байланысты қызметкерлердің жауапкершілігі еңбек шартында және лауазымдық нұсқаулықтарда белгіленген.

252.ҚР қолданыстағы заңнамасына қайшы келмейтін бөлігінде тіркеу орталығы:

1) тіркеу куәлігін шығаруға немесе кері қайтарып алуға өтініштерде қате, жаңылыстыратын немесе көрінеу жалған ақпаратты растау;

2) тіркеу куәлігін шығаруға немесе кері қайтарып алуға арналған өтініште көрсетілуге жататын елеулі фактілерді байқаусызда немесе қасақана жасыру.

253.ҚР қолданыстағы заңнамасына қайшы келмейтін бөлігінде тіркеу куәліктерінің иелері:

1) тіркеу куәлігін шығаруға немесе кері қайтарып алуға өтініште қате, жаңылыстыратын немесе көрінеу жалған ақпарат беру;

2) тіркеу куәлігін шығаруға немесе кері қайтарып алуға арналған өтініште көрсетілуге жататын елеулі фактілерді байқаусызда немесе қасақана жасыру;

3) өзінің бөлінген атауының құрамында зияткерлік меншік құқығын бұзатын атауларды үшінші тұлғаларды пайдалану.

254.ҚР қолданыстағы заңнамасына қайшы келмейтін бөлігінде тіркеу куәліктерін пайдаланушылар (сенім білдіруші Тараптар):

1)тіркеу куәліктерін пайдаланушының (сенім білдіруші Тараптың) міндеттемелерін бұзуына байланысты жіберілген тіркеу куәлігіне негізсіз сенім;

2) тіркеу куәлігінің қолданылу мерзімдері мен мәртебесін айқындау мақсатында оны тексеру жөнінде шаралар қолданбау (кері қайтарып алынды/кері қайтарылмады).

255.Қағидалардың тиісінше орындалуы үшін жауапкершілік Қағидалардың 251-тармағында көрсетілген КО қызметкерлері мен басшыларына жүктеледі.

256.Қағидаларды тиісінше орындамағаны үшін жауапкершілік Қағидалардың 251-тармағында көрсетілген КО қызметкерлері мен басшыларына жүктеледі.

257.263. Цифрлық даму бөлімшесінің басшысы ішкі бақылау саясатын және банкте ішкі бақылауды жүзеге асыру рәсімін регламенттейтін Банктің ІҚ ережелеріне сәйкес тиімді ішкі бақылауды ұйымдастыруға және қолдауға жауапты болады.

258.Қағидалардың 251-тармағында көрсетілген КО басшылары мен қызметкерлері, КО қызметіне қатысатын, ішкі бақылау саясатын және Банкте ішкі бақылауды жүзеге асыру рәсімін регламенттейтін Банктің ІҚ ережелеріне сәйкес ішкі бақылауды ұйымдастыруға және жүзеге асыруға жауапты болады.

259.Қағидалардың 251-тармағында көрсетілген, КО қызметіне қатысатын КО басшылары мен қызметкерлері өздерінің функционалдық міндеттерін орындау кезінде мүдделер қақтығысын болдырмау қағидатын қатаң ұстануға міндетті және банктегі мүдделер қақтығысын басқару саясатын регламенттейтін Банктің ІҚ ережелерін сақтауға жауапты болады. Мүдделер қақтығысы туындаған жағдайда КО басшылары мен қызметкерлері бұл туралы тікелей басшыға және комплаенс-тәуекелді басқару жөніндегі бөлімшеге хабарлайды.

12-тарау. Құпиялылық

260.Қағиданың 3-тарауына сәйкес КО қоймасында қолжетімді ақпаратты қоспағанда, КО қызметі туралы өзге ақпарат белгілі бір мәліметтерді банктік/коммерциялық құпияға жатқызу мәселелері бойынша Банктің ІҚ-на сәйкес құпия ретінде жіктеледі. Бұл құжат АКИ

қатысушыларының жауапкершілігін және оларды көрсетілген ақпаратпен КО ға жүгіну тәртібін регламенттейді.

261.Тіркеу куәлігін шығаруға арналған өтініш өтініш берушінің дербес деректерді жинауға және өңдеуге ҚР заңнамасына сәйкес дербес деректер және оларды қорғау мәселелері бойынша келісімін растайды, оның ішінде КО-ға өтініш берушінің тіркеу куәліктерін және олардың қоймадағы мәртебесі туралы ақпаратты жариялауға рұқсат береді.

13-тарау. Қорытынды ережелер

262.Қағида 050059, Алматы қ., Медеу ауданы, Нұрсұлтан Назарбаев даңғылы, 242 мекенжайында орналасқан КО өзектендіріледі.

263.Құжатты өзектендіру мәселелері бойынша Байланысатын тұлға - КО басшысы, 050059, Алматы қ., Медеу ауданы, Нұрсұлтан Назарбаев даңғылы, 242 үй, +7(727) 331 26 04 (ішкі ____), _____@jusan.kz.

264.Қағидалар саясатқа сәйкес қолданылады.

265.Егер Басқарма шешімімен өзге мерзім белгіленбесе, ереже басқарма бекіткен күннен бастап 5 (бес) жұмыс күні өткен соң жарияланады.

266.Қағидалар, оның ішінде оларға өзгерістер мен толықтыруларды ескере отырып, Банктің корпоративтік интернет-ресурсында жарияланған күнінен бастап күшіне енеді. Қағидамен реттелмеген ережелер ҚР және Банктің ІҚ заңнамасымен реттеледі.

267.ҚР заңнамасы өзгерген және ережелердің жекелеген ережелерінде ҚР заңнамасына қайшылықтар туындаған жағдайда, Қағидалардың мұндай ережелері күшін жояды және банк қызметкерлері ережелерді тиісті өзектендіргенге дейін өз қызметінде ҚР заңнамасын басшылыққа алады.

268.Қағидаға өзгерістер мен толықтырулар енгізілген жағдайда, Қағиданы Банк Басқармасы жаңа редакцияда бекітеді.

269.Қағидалардың жаңа бекітілген редакциясын жариялау КО шығарған барлық тіркеу куәліктерінің пайдаланушылары, олардың иелерін қоса алғанда, оның күшіне енуі туралы ресми хабарлама болып табылады.

270.Қағидалардың жаңа редакциясы жарияланған күннен бастап, егер бекітуші шешімнің өтпелі ережелерінде өзгеше көзделмесе, өзгерістер мен толықтырулар пайдаланушылар өздерінің иелерін қоса алғанда, КО шығарған барлық тіркеу куәліктерін қолдану үшін міндетті болады.

271.Жарияланатын өзгерістер мен оларға толықтыруларды ескере отырып, қағидалар Банктің корпоративтік интернет-ресурсында Қағидалардың жаңа редакциясы жарияланған сәтке дейін күшін сақтайды.

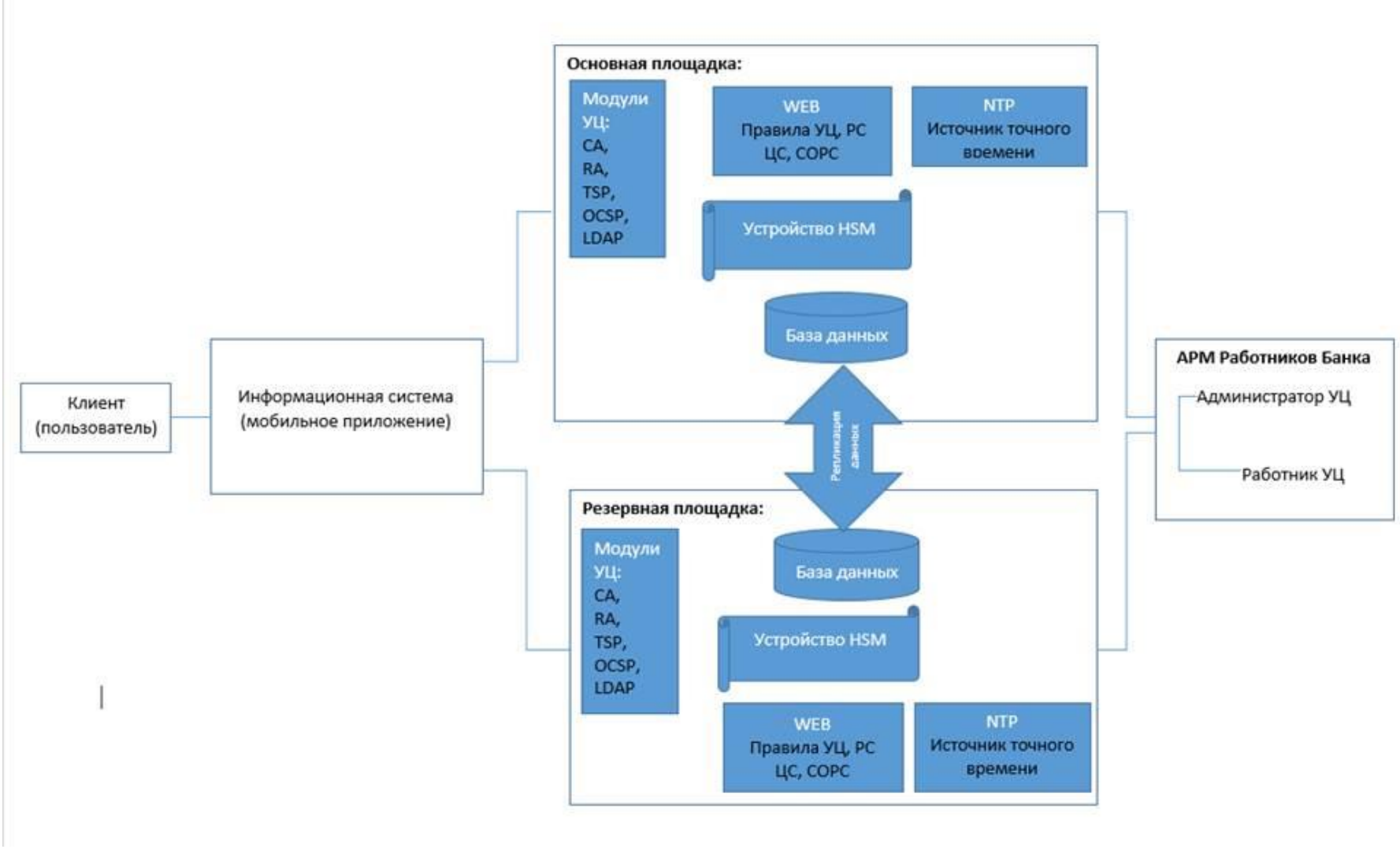
272.Қағидалар жойылған жағдайда КО шығарған тіркеу куәліктерін пайдаланатын АЖ қатысушылары тіркеу куәліктерінің қолданылу кезеңі өткенге дейін саясаттың талаптарымен байланысты болып қалады.

273.Егер Қағида ережелерінің бір бөлігін сот немесе уәкілетті мемлекеттік орган қолданылмайды деп таныған жағдайда, олардың қалған бөлігі күшін сақтайды.

274.Еңсерілмейтін күш (форс-мажор) мән-жайлары туындаған жағдайда АКИ қатысушылары: куәландырушы орталық, тіркеу куәліктерінің иелері мен пайдаланушылары (иелері мен сенім білдіруші Тараптар) - олардың арасында қолданылатын шарттардың тиісті ережелерін басшылыққа алады (бар болса).

Куәландырушы орталық қызметінің қағидаларына
1-қосымша

Куәландырушы орталықтың модульдерінің (компонентінің) өзара іс-қимыл схемасы



Куәландырушы орталық модульдерінің (компонент) өзара іс-қимыл схемасына
ТҮСІНДІРМЕ ЖАЗБА
Компоненттердің өзара іс-қимылы (негізгі және резервтік орталық)

Сертификаттау орталығының модульдерінің КО қоймасымен тіркеу куәліктерін жариялау және іздеу үшін өзара іс-қимылы LDAP хаттамасы бойынша ҚТКТ жүзеге асырылады.

Барлық КО модульдері NTP протоколы бойынша нақты уақыт көзінен алынған бір уақытты пайдаланады.

КО модульдерінің өзара іс-қимылының қауіпсіздігі ҚР СТ 1073-2007 сәйкес қауіпсіздіктің 3 (үшінші) деңгейіне сәйкес келетін "Тұмар-CSP" сертификатталған криптографиялық ақпаратты қорғау құралын пайдаланумен қамтамасыз етіледі.

КО жабық кілттерін сақтау және қауіпсіздігін қамтамасыз ету үшін ҚР СТ 1073-2007 сәйкес қауіпсіздіктің 2 (екінші) деңгейіне сәйкес HSM қорғалған бағдарламалық-аппараттық кешендері пайдаланылады.

Жүйеге кіретін барлық желілік трафикті басқаратын және сүзетін желіаралық экрандар қатысады.

Деректер орталығының жұмыс және резервтік серверлері арасындағы өзара әрекеттесу

Деректерді сақтау және басқару PostgreSQL ДҚБЖ арқылы қамтамасыз етіледі

Негізгі және резервтік орталықтар арасында нақты уақыт режимінде ДҚБЖ деректердің репликациясы орындалады, бұл жүйенің ақауларға төзімділігін арттырады.

Қайталанатын деректерді қорғау TLS протоколын қолдана отырып шифрлау арқылы қамтамасыз етіледі.

Пайдаланушылардың куәландырушы орталықпен өзара іс-қимылы

Тіркеу куәлігінің иесі және сенім білдіруші тарап КО сервистерімен тікелей өзара іс-қимыл жасамайды.

Өзара әрекеттесу LDAP және HTTP (S) хаттамаларын қолдана отырып, LDAP қоймасымен және сертификаттау орталығының модульдерімен өзара әрекеттесу мүмкіндігі бар мақсатты (қызмет көрсетілетін) тіркеу орталықтары арқылы жүзеге асырылады.

КО қызметкерлерінің куәландырушы орталық модульдерімен өзара іс-қимылы

Объектілік саясат идентификаторында көрсетілген КО қызметкерлерінің Сертификаттау орталығының модульдерімен өзара іс-қимылы LDAP және HTTP(S) хаттамаларын пайдалана отырып, мамандандырылған бағдарламалық қамтамасыз ету арқылы жүзеге асырылады.

Жоғарыда көрсетілген КО қызметкерінің жұмыс орнынан Сертификаттау орталығының модульдеріне қол жеткізу белгілі бір қасиеттері бар қолданыстағы тіркеу куәлігі болған жағдайда ғана мүмкін болады.

Сонымен қатар, қауіпсіздік желіге кіруді тек белгілі бір IP мекенжайлар жиынтығымен шектеу арқылы қамтамасыз етіледі.

Куәландырушы орталық қызметінің қағидаларына
2-қосымша

Схемы электронной цифровой подписи с данными о применяемых алгоритмах криптографических преобразований и другими исходными данными (основными требованиями) по реализации процесса формирования электронной цифровой подписи и требованиями к отдельным параметрам и удостоверяющему центру