



"Альфа-Банк" ЕБ АҚ Басқармасының
(2021 жылғы 23 қарашадағы №320/21)
шешімімен
Б е к і т і л д і

2021 жылғы 28 желтоқсанда
күшіне енді

**«Альфа-Банк» ЕБ АҚ-ның
Куәландырушы орталық ретіндегі қызметінің
Е Р Е Ж Е Л Е Р І
(2.0.0 редакциясы)**

Алматы қ.

2021 ж.

М А З М Ұ Н Ы:

1 бөлім. КІРІСПЕ.....	5
1.1.параграф. ЖАЛПЫ ҚАҒИДАЛАР	5
1.2 параграф. ҚҰЖАТ АТАУЫ ЖӘНЕ АТРИБУТТАРЫ.....	5
1.3 параграф. БАНКІНІҢ АШЫҚ КІЛТТЕР ИНФРАҚҰРЫЛЫМЫНЫҢ ҚАТЫСУШЫЛАРЫ	6
1.4 параграф. ТІРКЕУ КУӘЛІКТЕРІНІҢ МАҚСАТЫ	6
1.5 параграф. ҚҰЖАТТЫ БАСҚАРУ	7
1.6 параграф. ГЛОССАРИЙ.....	7
2 бөлім. ҚОЙМА ЖӘНЕ ОНДАҒЫ ДЕРЕКТЕРДІ ЖАРИЯЛАҒАНЫ ҮШІН ЖАУАПКЕРШІЛІК.....	10
2.1 параграф. ҚОЙМА.....	10
2.2 параграф. ҚОЙМАДА ТІРКЕУ КУӘЛІКТЕРІ ТУРАЛЫ АҚПАРАТТЫ ЖАРИЯЛАУ	10
2.3параграф. ҚОЙМАДАҒЫ ДЕРЕКТЕРДІ АКТУАЛДАНДЫРУ КЕЗЕҢДІЛІГІ.....	10
2.4 параграф. ҚОЙМАҒА ҚОЛ ЖЕТКІЗУДІ БАҚЫЛАУ	11
3 бөлім. СӘЙКЕСТЕНДІРУ ЖӘНЕ АУТЕНТИФИКАЦИЯ.....	11
3.1 параграф. АТТАРҒА ҚОЙЫЛАТЫН ТАЛАПТАР	11
3.2параграф. БІРДЕЙЛІКТІ БАСТАПҚЫ ТЕКСЕРУ	12
4 бөлім. ТІРКЕУ КУӘЛІКТЕРІНІҢ ӨМІРЛІК ЦИКЛДЕРІНЕ ҚОЙЫЛАТЫН ОПЕРАЦИЯЛЫҚ ТАЛАПТАР	12
4.1 параграф. ТІРКЕУ КУӘЛІКТЕРІН ШЫҒАРУҒА ӨТІНІШ.....	12
4.2параграф. ТІРКЕУ КУӘЛІКТЕРІН ШЫҒАРУҒА ӨТІНІШТЕРДІ ӨҢДЕУ	12
4.3параграф. ТІРКЕУ КУӘЛІКТЕРІН ШЫҒАРУ	13
4.4 параграф. ТІРКЕУ КУӘЛІКТЕРІН ҚАБЫЛДАУ.....	13
4.5 параграф. КІЛТ ЖҰПТАРЫ МЕН ТІРКЕУ КУӘЛІКТЕРІН ПАЙДАЛАНУ	14
4.6 параграф. ТІРКЕУ КУӘЛІКТЕРІНДЕГІ ҚОЛДАНУ МЕРЗІМІН ЖАҢАЛАУ	15
4.7 параграф. ТІРКЕУ КУӘЛІКТЕРІНДЕГІ КРИПТОГРАФИЯЛЫҚ КІЛТТЕРДІ АУЫСТЫРУ	15
4.8 параграф. ТІРКЕУ КУӘЛІКТЕРІНДЕГІ ДЕРЕКТЕРДІ ӨЗГЕРТУ	15
4.9 параграф. ТІРКЕУ КУӘЛІКТЕРІН КЕРІ ҚАЙТАРЫП АЛУ	15
5 бөлім. ФИЗИКАЛЫҚ, ОПЕРАЦИЯЛЫҚ ЖӘНЕ БАСҚАРУШЫ БАҚЫЛАУЛАР ...	17
5.1 параграф. ФИЗИКАЛЫҚ БАҚЫЛАУ	17

5.2 параграф. ОПЕРАЦИЯЛЫҚ БАҚЫЛАУ	17
5.3 параграф. ҚЫЗМЕТКЕРЛЕРДІ БАҚЫЛАУ	17
5.4 параграф. БАҚЫЛАУ ХАТТАМАЛАУЫНЫҢ ПРОЦЕДУРАЛАРЫ	18
5.5 параграф. АРХИВ ЖҮРГІЗУ	18
5.6 параграф. КУӘЛАНДЫРУШЫ ОРТАЛЫҚТЫҢ КРИПТОГРАФИЯЛЫҚ КІЛТТЕРІН АУЫСТЫРУ	19
5.7 параграф. ТӨТЕНШЕ ОҚИҒАЛАР НЕМЕСЕ ӘШКЕРЕ БОЛУ ЖАҒДАЙЫНДА ЖҰМЫС ІСТЕУДІ ҚАЛПЫНА КЕЛТІРУ	19
5.8 параграф. КУӘЛАНДЫРУШЫ ОРТАЛЫҚ ЖҰМЫСЫНЫҢ ТОҚТАУЫ.....	20
6 бөлім. ҚАУІПСІЗДІКТІ ТЕХНИКАЛЫҚ БАҚЫЛАУ	20
6.1 параграф. КРИПТОГРАФИЯЛЫҚ КІЛТТЕРДІ.....	20
ГЕНЕРАЦИЯЛАУ ЖӘНЕ ОРНАТУ	20
6.2 параграф. ЖАБЫҚ КРИПТОГРАФИЯЛЫҚ КІЛТТЕРДІ ҚОРҒАУ ЖӘНЕ КРИПТОГРАФИЯЛЫҚ МОДУЛЬДЕРДІ ИНЖЕНЕРЛІК БАҚЫЛАУ	21
6.3 параграф. КРИПТОГРАФИЯЛЫҚ КІЛТТЕРДІ БАСҚАРУДЫҢ ӨЗГЕ АСПЕКТІЛЕРІ.....	22
6.4 параграф. АКТИВТЕУ ДЕРЕКТЕРІ	22
6.5 параграф. ЕСЕПТЕУ РЕСУРСТАРЫНЫҢ ҚАУІПСІЗДІГІН БАҚЫЛАУ	23
6.6 параграф. ДАМУДЫ ЖӘНЕ ҚАУІПСІЗДІКТІ БАСҚАРУДЫ БАҚЫЛАУ	23
6.7 параграф. ЖЕЛІ ҚАУІПСІЗДІГІН БАҚЫЛАУ	23
6.8 параграф. УАҚЫТ БЕЛГІЛЕРІ	23
7 бөлім. ТІРКЕУ КУӘЛІКТЕРІНІҢ, СОРС ЖӘНЕ ОССР ПРОФИЛЬДЕРІ	23
7.1 параграф. ТІРКЕУ КУӘЛІГІНІҢ ПРОФИЛЬДЕРІ.....	23
7.2 параграф. КЕРІ ҚАЙТАРЫЛЫП АЛЫНҒАН ТІРКЕУ КУӘЛІКТЕРІ ТІЗІМІНІҢ ПРОФИЛЬДЕРІ.....	24
7.3 параграф. ОССР СЕРВИСІНІҢ ПРОФИЛІ.....	24
8 бөлім. ҚЫЗМЕТТІ ТЕКСЕРУ	24
9 бөлім. ӨЗГЕ СҰРАҚТАР	24
9.1 параграф. ТАРИФТЕР	24
9.2 параграф. ЖАУАПКЕРШІЛІК	25
9.3 параграф. АҚПАРАТТЫҢ ҚҰПИЯЛЫҒЫ.....	25
9.4 параграф. ҚАТЫСУШЫЛАРДЫҢ ДЕРБЕС ДЕРЕКТЕРІН ҚОРҒАУ	25
9.5 параграф. ЗИЯТКЕРЛІК МЕНШІК ҚҰҚЫҒЫ.....	25
9.6 параграф. КЕПІЛДІКТЕР ЖӘНЕ КУӘЛАНДЫРУЛАР	26
9.7 параграф. КЕПІЛДІКТЕН БАС ТАРТУ	26
9.8 параграф. ЖАУАПКЕРШІЛІКТІ ШЕКТЕУ	27

9.9 параграф. ӨТЕМДЕР	27
9.10 параграф. КҮШНЕ ЕНУІ ЖӘНЕ ҚОЛДАНЫЛУЫНЫҢ ТОҚТАУЫ	27
9.11 параграф. ЖЕКЕ ХАБАРЛАМА ЖӘНЕ ҚАТЫСУШЫЛАРМЕН БАЙЛАНЫС ..	27
9.12 параграф. ӨЗГЕРТУЛЕР МЕН ТОЛЫҚТЫРУЛАР.....	27
9.13 параграф. ДАУЛАРДЫ ШЕШУ	27
9.14 параграф. ЮРИСДИКЦИЯ.....	28
9.15 параграф. ҚОЛДАНЫСТАҒЫ ЗАҢНАМАҒА СӘЙКЕСТІК	28
9.16 параграф. ӨЗГЕ ҚАҒИДАЛАР	28
1 қосымша.....	29
2 қосымша.....	31

1 бөлім. КІРІСПЕ

1.1. параграф. ЖАЛПЫ ҚАҒИДАЛАР

1. «Альфа-Банка» ЕБ АҚ-ның куәландырушы орталық ретіндегі осы Қызмет ережелері (әрі қарай – Ережелер) «Альфа-Банка» ЕБ АҚ-ның Куәландырушы орталығының (әрі қарай – Куәландырушы орталық/Банк) жұмыс істеуін қамтамасыз ету мақсатында Қазақстан Республикасының электрондық құжат және электрондық цифрлық қолтаңба сұрақтары бойынша құқықтық актілерінің талаптарына сәйкес әзірленген және оның жұмыс істеу тәртібін анықтайды.
2. Ережелер RFC 3647 «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework» (X.509 форматындағы ашық кілттер интернет инфрақұрылымындағы сертификаттар саясаты және практикасы құжаттарының құрылымы) халықаралық салалық кеңестерін ескере отырып әзірленді.
3. Ережелер «Альфа-Банк» ЕБ АҚ Куәландырушы орталығының тіркеу куәліктерін қолдану саясаты (әрі қарай – Тіркеу куәліктері саясаты) анықтаған сервистер жиынтығын қамтамасыз ету кезіндегі Куәландырушы орталық жүзеге асыратын шараларды анықтайды және тіркеу куәліктерін шығаруды, басқаруды және оларды кері қайтарып алуды қамтиды, бірақ олармен шектелмейді.
4. Тіркеу куәліктері саясаты Куәландырушы орталық шығаратын тіркеу куәліктерінің түрлерін, негізгі принциптерін және Банкінің ақпараттық қауіпсіздігінің типтік талаптарымен біріктірілген мүдделі ақпараттық жүйелерде оларды қолданудың жалпы талаптарын анықтайды, бұл осы тіркеу куәліктерін пайдаланатын ақпараттық жүйелердегі сенімнің белгілі бір деңгейіне кепілдік береді.
5. Ережелердің Тіркеу куәліктері саясатынан айырмашылығы олар тәртіп пен процедураны анықтайды, оған сәйкес:
 - 1) Куәландырушы орталық қызметін атқарады (сервистер жұмыс істейді);
 - 2) ашық кілттер инфрақұрылымы ядросының қауіпсіздігі мен басқарылуы қамтамасыз етіледі.
6. Куәландырушы орталықтың сервистерін пайдаланатын Банкінің ақпараттық жүйесіне қатысушы тіркеу куәлігін шығару өтінішіне (кез келген нысанда: қағаздағы, электрондық түрдегі немесе Банкінің ақпараттық жүйесінде сақталатын электрондық өтінім нысанындағы құжат) қол қойған сәттен бастап қатысушы үшін өтініште сілтемесі көрсетілген Тіркеу куәліктері саясатының және Ережелердің оған қолданылатын талаптарын орындау міндетті болады.
7. Ереже сондай-ақ Тіркеу куәліктерінің саясатына сәйкес куәландырушы орталық шығаратын тіркеу куәліктерінің түрлерін шығаруға және одан ары қарай қызмет көрсетуге байланысты тексеру процедураларын айқындайды.
8. Куәландырушы орталықтың жазылушылар үшін шығаратын тіркеу куәліктері түрлерінің толық тізбесі оларды сәйкестендіретін белгілерді (профильдерді) көрсете отырып, Тіркеу куәліктері саясатының 1.1-параграфында анықталған.

1.2 параграф. ҚҰЖАТ АТАУЫ ЖӘНЕ АТРИБУТТАРЫ

9. Құжат ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілті орган шығарған Куәландырушы орталықтарды аккредитациялау сұрақтары бойынша құқықтық акт¹ талап еткендей «Альфа-Банка» ЕБ АҚ-ның куәландырушы орталық ретіндегі Қызмет ережелері» деп аталады,

¹ Ереже бекітілген күні Қазақстан Республикасы Цифрлық даму, инновация және аэроғарыш өнеркәсібі министрлігінің 2020 жылғы 1 маусымдағы № 224/НҚ “Куәландырушы орталықтарға аккредитация жүргізу қағидаларын бекіту туралы» бұйрығы қолданыста болды.

-
-
10. Құжат редакциясы 2.0.0.
 11. Осы редакциядағы Ережелер қолданысқа Банк Басқармасының 2021 жылғы 23 қарашадағы № 320/21 хаттамалық шешімімен қолданысқа енгізілді.
 12. Ережелердің қолданыстағы редакциясы Интернет желісіндегі Банкінің ресми ақпараттық ресурсында <https://alfabank.kz/pki/#DPP> адресі бойынша жарияланады.
 13. Ережелер 1.2.398.3.21.1.2.1 объектілік сәйкестендіргіші беріле отырып, халықаралық объектілік сәйкестендіргіштер ағашына тіркелген.

1.3 параграф. БАНКІНІҢ АШЫҚ КІЛТТЕР ИНФРАҚҰРЫЛЫМЫНЫҢ ҚАТЫСУШЫЛАРЫ

14. Куәландырушы орталық – Банкінің ашық криптографиялық кілттің жабық криптографиялық кілтке сәйкестігін куәландыратын, сондай-ақ өзі шығарған тіркеу куәлігінің шынайылығы мен жарамдылығын растайтын құрылымдық бөлімшесі².
15. Куәландырушы орталықтың Тіркеу орталығы –өз штатында тіркеу куәліктерін шығаруға немесе оларды кері қайтарып алуға құжаттар қабылдауға, өтініш берушілерді сәйкестендіруге, тиісті сұраныстарды куәландыруға және оларды Куәландырушы орталыққа жіберуге, сонымен қатар өтініш берушілерге олардың дайын тіркеу куәліктеріне қол жеткізу үшін қажетті деректерді беруге уәкілетті қызметкерлері бар Банкінің бөлімшесі.
16. Тіркеу куәлігінің иесі (немесе Куәландырушы орталықтың жазылушысы) - жеке тұлға немесе заңды тұлға, ол атына тіркеу куәлігі берілген субъект ретінде өзінің уәкілетті өкілінің атынан әрекет етеді және тіркеу куәлігінде көрсетілген ашық кілтке сәйкесетін жабық кілтті заңды түрде иелене алады.
17. Сенім білдіруші тараптар (немесе тіркеу куәліктерін пайдаланушылар) – тіркеу куәліктерінің барлық иелері, немесе Куәландырушы орталық шығарған тіркеу куәліктеріне және/немесе электрондық цифрлық қолтаңбалары бар электрондық құжаттарға сүйеніп әрекет ететін кез келген басқа субъектілер, ол цифрлық қолтаңбалардың түпнұсқалығы осы тіркеу куәліктерінің көмегімен тексеріледі.

1.4 параграф. ТІРКЕУ КУӘЛІКТЕРІНІҢ МАҚСАТЫ

18. Куәландырушы орталық Тіркеу куәліктері саясаты 1.1 параграфына сәйкес әртүрлі мақсаттағы тіркеу куәліктерін және осыған сәйкес әртүрлі профильдер шығарады, олар “keyUsage” және “extendedKeyUsage” кеңейтілімдерінде көрсетіледі.
19. “keyUsage” және “extendedKeyUsage” кеңейтілімдері мәнінің толық тізбесі клиенттік тіркеу куәліктерінде Интернет желісіндегі Банкінің ақпараттық ресурсында <https://alfabank.kz/pki/#DPP> адресі бойынша келтірілген.
20. Бұдан өзге, "certificatePolicies" кеңейтілімі бар Куәландырушы орталық шығаратын тіркеу куәліктері үшін Тіркеу куәліктері саясатының 1.4 параграфына сәйкес жол берілетін қолдану саласы көрсетілген кеңейтілімде бекітілген саясаттың объектілік сәйкестендіргіштерімен қосымша шектеледі.
21. Клиенттік тіркеу куәліктеріндегі саясаттың объектілік сәйкестендіргіштерінің тізбесі Интернет желісіндегі Банкінің <https://alfabank.kz/pki/#OIPS> адресі бойынша ресми ақпараттық ресурсында келтірілген. Тізбені жаңа объектілік сәйкестендіргіштерінің тіркелуіне қарай Қазақстан Республикасының уәкілетті мемлекеттік органы толықтырады.

² Ережелер бекітілген күні көрсетілген міндетті Банк Басқармасы Төрағасы блогының Ақпараттық қауіпсіздік департаментінің куәландырушы орталығының басқармасы шешеді.

1.5 параграф. ҚҰЖАТТЫ БАСҚАРУ

22. Ережелерді А15G5M8, Алматы қ., Айманов көшесі, 140 үй, Б2 блогы мекенжайында орналасқан Куәландырушы орталық актуалдандырады.
23. Құжатты актуалдындыру сұрақтары бойынша байланысу тұлғасы – Куәландырушы орталықтың бас талдаушысы, А15G5M8, Алматы қ., Айманов көшесі, 140 үй, Б2 блогы, +7 (727) 259-05-01 (іш. 4758), amakhnin@alfabank.kz.
24. Ережелер Тіркеу куәліктері саясатына сәйкес қолданылады³.
25. Ережелерге өзгертулер мен толықтыруларды жаңа редакция нысанында, немесе Ережелердің ағымдағы редакциясына өзгертулер мен толықтырулар тізбесі нысанында Куәландырушы орталық дайындайды.
26. Ережелерге өзгертулер мен толықтырулар бекітер алдында ішкі процедураларға сәйкес Банкінің мүдделі бөлімшелерінің және лауазымды тұлғалардың келісуінен өтеді⁴.
27. Ережелерге өзгертулер мен толықтырулар Банк Басқармасының хаттамалық шешімімен бекітіледі.
28. Ережелерге жасалған барлық өзгертулер мен толықтырулар Интернет желісіндегі Банкінің ресми ақпараттық ресурсында жарияланады.
29. Ережелерді жаңа бекітілген редакцияда жариялау Куәландырушы орталық шығарған тіркеу куәліктерін пайдаланушылардың барлығы үшін, олардың иелерімен қоса, оның күшіне енгені туралы ресми хабарлама болып табылады.
30. Ережелерге енгізілген өзгертулер мен толықтырулар жарияланған күннен бастап, егер бекітуші шешімнің өтпелі қағидаларында өзгеше қарастырылмаған болса, өзгертулер мен толықтырулар Куәландырушы орталық шығарған тіркеу куәліктерін пайдаланушылардың барлығы үшін, олардың иелерімен қоса, қолдану үшін міндетті болады.

1.6 параграф. ГЛОССАРИЙ

31. Ережелерде келесі түсініктер қолданылады:
 - 1) аутентификация – тұлғаның (заттың) өзін кім деп атайтыны (не деп атайтыны) болып табылатынын тексеруге арналған осы процесті жүзеге асыратын қауіпсіздік процесі немесе сервисі.
 - 2) Банк – «Альфа-Банк» ЕБ АҚ;
 - 3) Активтеу деректері – криптографиялық операцияларды орындау үшін қажетті және қорғауды қажет ететін криптографиялық кілттерден басқа кез келген деректер: дербес сәйкестендіру нөмірлері (PIN), құпиясөз фразалары, бөлінген криптографиялық кілт компоненттері, биометриялық параметрлер және т.б.;
 - 4) халықаралық объектілік сәйкестендіргіштер ағашы – кез келген нақты немесе абстрактілі объектілерді бір типті анық барлығын қамтитын атаумен атайтын стандартталған ITU-T және ISO/IEC механизм (X.660), ол ерекше нысандағы үш иерархиялық ағаш көмегімен аттарды тіркеуге арналған (3 әртүрлі тамырдан

³ Ереже бекітілген күні Директорлар кеңесінің 2021 жылғы 03 шілдедегі №19 хаттамалық шешімімен бекітілген «Ішкі нормативтік құжаттарды әзірлеу, өзгерту және/немесе толықтыру және әрекетін тоқтату кезіндегі бөлімшелердің өзара әрекеті бойынша нұсқаулық» қолданыста болды. Альфа-Банк Қазақстан» ЕБ АҚ куәландырушы орталығының тіркеу куәлігін қолдану саясаты» (1.0.0. редакциясы) қолданыста болды.

⁴ Ереже бекітілген күні Банк басқармасының 2021 жылғы 29 маусымдағы №39 хаттамалық шешімімен бекітілген «Ішкі нормативтік құжаттарды әзірлеу, өзгерту және/немесе толықтыру және әрекетін тоқтату кезіндегі бөлімшелердің өзара әрекеті бойынша нұсқаулық» қолданыста болды.

-
-
- таралған), ондағы әр келесі түйін бүтінсанды нөмірге ие болады және оның өзінен таралатын бұтақтарды әрі қарай бөлуге және тіркеуге жауапты.
- 5) электрондық цифрлық қолтаңбаның жабық кілті – электрондық цифрлық қолтаңба құралдарын пайдалана отырып, электрондық цифрлық қолтаңба жасауға арналған электрондық цифрлық символдар реті.
 - 6) жабық криптографиялық кілт – ашық кілті бар криптожүйедегі тек жазылушыға белгілі кілт жұбының бір кілті⁵;
 - 7) сәйкестендіру – Ережелер мәнмәтінінде жеке немесе заңды тұлғаның (осы тұлғаның шын мәнінде айқындалған анық өмірде бар тұлға болып табылатынын көрсететін) сәйкестігін белгілейтін процесс (немесе процесс нәтижесі) және ол екі кезеңнен тұрады:
 - ұсынушы тұлға ұсынған аттың анық өмірде бар тұлғамен сәйкестігін анықтау және
 - белгілі бір атпен әлденеге қол жеткізу үшін жүгінген тұлғаның шын мәнінде өзі атаған атқа ие тұлға болып табылатынын анықтау (аутентификация);
 - 8) ашық кілттер инфрақұрылымы – бірлесе келе көмегімен көрсетілген міндеттер шешілетін ашық кілттерді басқаруды өз бетінше қамтамасыз етуге қабілетті ашық кілті бар криптожүйе негізінде криптографиялық міндеттерді шешу (аутентификация, шифрлеу, біртұтастығы мен дәлелділігін бақылау) үшін пайдаланылатын таратылып бөлінген қызметтер мен компоненттердің күші мен құралдарының жиынтығы (техникалық, материалдық, адамдар және басқа);
 - 9) криптографиялық кілттердің әшкере болуы – криптографиялық кілттер иесінің нақты криптографиялық кілттердің осы кілттердің көмегімен қорғалатын ақпараттың қауіпсіздігін қамтамасыз ететіне сенімінің жоғалуы;
 - 10) негізгі ақпаратты тасымалдаушы – Ережелер мәнмәтінінде криптографиялық кілттерді электронды түрде сақтауға қабілетті алынбалы машиналық ақпараты тасымалдаушы (мамандандырылған аппараттық токен, жад картасы, қатты диск және т.б.);
 - 11) объектілік сәйкестендіргіш – ағаштың тамырынан осы түйінге қарай тәртіпке келтірілген бүтінсанды мәндер тізімі нысанындағы халықаралық объектілік сәйкестендіргіштер ағашына бірімәнді ат беретін сәйкестендіргіш;
 - 12) электрондық сандық қолтаңбаның ашық кілті – кез келген тұлғаға қол жетімді және электрондық құжатта электрондық сандық қолтаңбаның түпнұсқалылығын растауға арналған электрондық цифрлық символдар реті;
 - 13) ашық криптографиялық кілт – ашық кілтті криптожүйелердегі кілт жұбының көпшілікке белгілі кілті⁶;
 - 14) тіркеу куәліктерін қолдану саясаты (сонымен қатар Тіркеу куәліктерінің саясаты деп те аталады) – ол ақпараттық қауіпсіздіктің жалпы талаптары бар қосымшалардың белгілі бір қауымдастығында (класында) тіркеу куәлігінің қолданымдылығын анықтайтын тақырып қойылған ережелер жинағы болып табылатын нормативтік құжат.
 - 15) куәландырушы орталық қызметінің ережелері - куәландырушы орталықтың негізгі бизнес-процестерінің барысымен қоса, тіркеу куәліктерін қолдану саясатына сәйкес жүзеге асырылатын куәландырушы орталықтың негізгі қызметін ұйымдастыру тәртібін анықтайтын нормативтік құжат;

⁵ Жабық электрондық цифрлық қолтаңба кілттері жабық криптографиялық кілттердің бір түрі болып келеді.

⁶ Ашық электрондық цифрлық қолтаңба кілттері ашық криптографиялық кілттердің бір түрі болып келеді.

-
-
- 16) тіркеу куәлігі – электрондық цифрлық қолтаңбаның Қазақстан Республикасының «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Заңында белгіленген талаптарға сәйкестігін растау үшін куәландырушы орталық беретін электрондық құжат;
 - 17) ашық (криптографиялық) кілт сертификаты (әрі қарай – сертификат) – жазылушының қосымша ақпаратпен бірге осы кілтті және жазылушыны сәйкестендіруші ашық криптографиялық кілті, олардың түпнұсқалығы мен өзара байланысы Куәландырушы орталықтың жабық криптографиялық кілтімен қалыптастырылған электрондық цифрлық қолтаңбамен куәландырылған⁷;
 - 18) кері қайтарылып алынған тіркеу куәліктерінің тізімі (КТКТ) – қолданылуы тоқтатылған тіркеу куәліктері туралы мәліметтер, олардың сериялық нөмірлері, кері қайтарып алу күні мен себебі берілген тіркеу куәліктері тіркелімінің бөлігі;
 - 19) ақпаратты криптографиялық қорғау құралы (немесе АКҚК) – кілттерді криптографиялық түрлендіру, генерациялану, қалыптастыру, тарату немесе басқару алгоритмдерін іске асырушы құрал;
 - 20) электрондық цифрлық қолтаңба құралдары – электрондық цифрлық қолтаңбаны жасау және оның түпнұсқалылығын тексеру үшін пайдаланылатын бағдарламалық және техникалық құралдар жиынтығы;
 - 21) токен – Ережелер мәнмәтінінде уәкілетті тұлғаға Куәландырушы орталықтың жабық криптографиялық кілттерінің резервтік көшірмелерін қорғаулы сақтауды және аппараттық криптографиялық модульдерін (Hardware Security Module, HSM) баптау мақсатында берілетін физикалық құрылғы;
 - 22) ашық кілттер инфрақұрылымдарының қатысушылары – өздерінің уәкілетті өкілдері тұлғасында әрекет ететін жеке және заңды тұлғалар жиынтығы, ол уәкілетті тұлғалар келес рольдердің кез келгенін орындайды: тіркеу куәлігін пайдаланушының немесе оның иесінің (сенім білдіруші тарапың немесе жазылушының), тіркеу немесе куәландырушы орталықтың, – ашық кілттердің бір инфрақұрылымында;
 - 23) тіркеу куәліктері тізбесі – тіркеу куәлігінен басталатын тіркеу куәліктерінің тәртіпке келтірілген реті, ондағы электрондық цифрлық қолтаңба сенім жүктелген негізгі тіркеу куәлігінің көмегімен тексерілуі мүмкін, оны стандартталған алгоритмнің көмегімен сәтті өңдеу ашық криптографиялық кілттің реттіліктің қорытынды тіркеу куәлігінде, «subject» жолында көрсетілген тұлғаға тиесілігін растауға жол ашады.
 - 24) электрондық цифрлық қолтаңба (немесе ЭЦҚ) – электрондық цифрлық қолтаңба құралдарымен жасалған және электрондық құжаттың шынайылығын, оның

⁷ “Сертификат” түсінігі ITU-T X.509 “Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks” (Ақпараттық технология - Ашық жүйелердің өзара әрекеттесуі - Анықтамалық: ашық кілттер (криптографиялық) мен атрибуттар сертификаттарының құрылымы) халықаралық стандартына сәйкес енгізілген. Куәландырушы орталық Қазақстан Республикасының «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Заңына сәйкес шығаратын тіркеу куәліктері шығарылатын сертификаттардың бір түрі болып табылады. Сонымен қатар, Қазақстан Республикасының заңнамалық актілерінде «ашық (криптографиялық) кілт сертификаты» терминіне тең терминдер пайдаланылмайды. Осыған байланысты Ережелердің бүкіл мәтінінде Қазақстан Республикасының «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Заңында енгізілген «тіркеу куәліктері» термині Банкінің Куәландырушы орталығы шығаратын ашық (криптографиялық) кілттер сертификаттарының барлық ықтимал түрлерін жинақтайды, демек оны «өзге мақсаттағы ашық (криптографиялық) кілттердің тіркеу куәліктері және (немесе) сертификаттары» ретінде ашу қажет.

-
- тиесілілігі мен мазмұнының өзгермейтінін растайтын электрондық цифрлық символдар жиыны;
- 25) электрондық құжат – ақпарат электрондық-цифрлық нысанда берілген және ЭЦҚ арқылы куәландырылған құжат.

2 бөлім. ҚОЙМА ЖӘНЕ ОНДАҒЫ ДЕРЕКТЕРДІ ЖАРИЯЛАҒАНЫ ҮШІН ЖАУАПКЕРШІЛІК

2.1 параграф. ҚОЙМА

32. Куәландырушы орталықтың ақпараттық жүйесінің құрамдас бөлігі қойма болып табылады, оны Куәландырушы орталық өзінің негізгі сервистерін көрсету кезінде ақпарат анықтамалығы ретінде пайдаланады.
33. Қызмет көрсетілетін ақпараттық жүйелерге, Банкілер мен олардың пайдаланушыларына қоймадан ақпаратты оқуға қол жеткізу талаптары Ережелердің 2.4 параграфында көрсетілген.
34. Бұдан өзге, Куәландырушы орталық Интернет желісіндегі Банкінің ресми ақпараттық ресурсында <https://alfabank.kz/pki> адресі бойынша жариялайды:
- 1) Тіркеу куәліктерінің саясаты;
 - 2) Ережелер;
 - 3) Тіркеу куәліктері саясаты;
 - 4) Ережелер;
 - 5) Куәландырушы орталықтың тіркеу куәлігі;
 - 6) КЕРІ ҚАЙТАРЫЛЫП АЛЫНҒАН тіркеу куәліктерінің тізіміне қол жеткізуге арналған сілтемелер.
35. Ресурстың көрсетілген тарауы тіркеу куәліктерінің иелері мен пайдаланушыларына (жазылушылар мен сенім білдіруші тараптарға) хабарлау мақсатында Куәландырушы орталықтың өзге маңызды ақпаратын орналастыру үшін пайдаланылады.

2.2 параграф. ҚОЙМАДА ТІРКЕУ КУӘЛІКТЕРІ ТУРАЛЫ АҚПАРАТТЫ ЖАРИЯЛАУ

36. Куәландырушы орталықтың қоймасында онлайн режимінде қолданыстағы барлық тіркеу куәліктері («кері қайтарылып алынды» мәртебесі жоқ валидті тіркеу куәліктері), сонымен бірге кері қайтарылып алынған тіркеу куәліктерінің тізімі жарияланады.

2.3 параграф. ҚОЙМАДАҒЫ ДЕРЕКТЕРДІ АКТУАЛДАНДЫРУ КЕЗЕҢДІЛІГІ

37. Куәландырушы орталық шығарған әрбір тіркеу куәлігі қоймада автоматты түрде және дереу жарияланады (онлайн режимде).
38. Тіркеу куәлігін кері қайтарып алғанда қоймадан автоматты түрде кетіріледі және архивке көшіріледі.
39. Қоймада орналастырылған барлық тіркеу куәліктерінің қолданылу мерзімінің аяқталуын тексеру куәландырушы орталықтың ақпараттық жүйесінің тиісті баптауымен анықталған кесте бойынша тәулік сайын жүзеге асырылады.
40. Кез келген тіркеу куәлігі кері қайтарылып алынған жағдайда Куәландырушы орталық кері қайтарылып алынған тіркеу куәліктерінің жаңартылған тізімін автоматты түрде және тез арада (онлайн режимінде) қалыптастырады және қоймада жариялайды.
41. Кері қайтарып алу жағдайлары болмаған жағдайда кері қайтарылып алынған тіркеу куәліктерінің жаңа тізімдері Куәландырушы орталықтың ақпараттық жүйесінің тиісті

баптауымен анықталған кесте бойынша аптасына бір реттен сиретпей қалыптастырылады және шығарылады.

42. Қолданылу мерзімі өтіп кеткен кері қайтарып алынған тіркеу куәліктері кері қайтарып алынған тіркеу куәліктерінің тізімінен Куәландырушы орталықтың ақпараттық жүйесінің тиісті баптауымен анықталған кесте бойынша аптасына бір реттен сиретпей шығарылады.

2.4 параграф. ҚОЙМАҒА ҚОЛ ЖЕТКІЗУДІ БАҚЫЛАУ

43. Қоймадан деректерді оқу үшін банкінің қызмет көрсететін ақпараттық жүйелеріне Куәландырушы орталық тұрақты сипаттағы қандай да бір қосымша шектеулерсіз ақпараттық қауіпсіздік сұрақтары бойынша өтінімдер бойынша, Банктің ішкі нормативтік құжаттарында белгіленген тәртіпте қол жеткізу мүмкіндігін береді.
44. Қоймадан (қоймаға) деректер қосу, өзгерту үшін қол жеткізу мүмкіндігін Куәландырушы орталық уәкілетті тұлғалардың шектеулі аясына береді.
45. Қызмет көрсету деңгейінің тиісті параметрлерін сақтау қоймасына қол жеткізу сервисіне артық жүктеме түскен жағдайда Куәландырушы орталық сервистерді ұсынудағы кідірістің кибершабуылдарына, басқа қатерлеріне қарсы іс-қимылдың белсенді шаралары ретінде қолжетімділікті уақытша шектеуді автоматты түрде қолданады.
46. Қоймаға қол жеткізуді шектеу және бақылау Ақпараттық қауіпсіздік саясаты жүзеге асыратын Банкінің ішкі құжаттарымен реттеледі⁸.

3 бөлім. СӘЙКЕСТЕНДІРУ ЖӘНЕ АУТЕНТИФИКАЦИЯ

3.1 параграф. АТТАРҒА ҚОЙЫЛАТЫН ТАЛАПТАР

47. Куәландырушы орталық пайдаланатын субъектілерді атау ережелері барлық шығарылатын куәліктердегі иелерді (жазылушыларды) сәйкестендіруді қамтамасыз етеді.
48. Куәландырушы орталық шығарған барлық тіркеу куәліктеріндегі “Issuer” және “Subject” жолдарындағы субъектілердің аттары (DN-аттары) ITU-T X.520 халықаралық кеңестеріне сәйкес ерекшеленіп бөлінген аттар форматында көрсетіледі.
49. Куәландырушы орталық шығарған барлық тіркеу куәліктеріндегі “Issuer” жолының мазмұны мен атрибуттары бірдей, олардың мәндері Банкінің ресми ақпараттық ресурсында <https://alfabank.kz/pki/#PIS> адресі бойынша келтіріледі.
50. Куәландырушы орталықтың Тіркеу куәліктерін Негізгі куәландырушы орталық⁹ қызметінің сұрақтары бойынша реттегіштің құқықтық актісіне сәйкес Қазақстан Республикасының Негізгі куәландырушы орталығы берген.
51. Куәландырушы орталықтың жазылушыларының тіркеу куәліктеріндегі “Subject” жолдарының атрибуттарының жиыны және оларды толтыру ережелері Банкінің ресми ақпараттық ресурсында <https://alfabank.kz/pki/#PIS> адресі бойынша келтірілген.

⁸ Ақпараттық қауіпсіздік саясатының мәтіні келесі адрес бойынша Интернет желісіндегі Банкінің ресми ресурсында үнемі қолжетімді: https://alfabank.kz/uploads/up_docs/about_docs/10/ru/gNP54exu53BtRVTKYZ4KnaifYg3EMqSg.pdf келесі адрес бойынша Интернет желісіндегі Банкінің ресми ресурсында үнемі қолжетімді:

⁹ Ережелер бекітілген күні Қазақстан Республикасы Цифрлық даму, инновация және аэроғарыш өнеркәсібі министрлігінің 2020 жылғы 26 мамырдағы № 214/НҚ бұйрығымен бекітілген Қазақстан Республикасының Тіркеу куәліктерін беру, сақтау, кері қайтарып алу және Негізгі куәландырушы орталықтың электрондық цифрлық қолтаңбасының ашық кілтіннің тиесілілігі мен шынайылығын растау ережесі қолданыста болды.

3.2 параграф. БІРДЕЙЛІКТІ БАСТАПҚЫ ТЕКСЕРУ

52. Бірдейлікті бастапқы тексеру – бұл халықаралық салалық кеңестерге сәйкес бірінші тіркеу куәлігін шығару кезінде жазылушыға қатысты жүргізілетін сәйкестендіру және аутентификациялау процедураларының барынша толық нысаны.
53. Өтініш беруші өзі келген кезде тіркеу орталықтары ақпараттандыру саласындағы уәкілетті орган шығарған тіркеу куәліктерін беру, сақтау, кері қайтарып алу сұрақтары бойынша құқықтық актіге сәйкес жазылушының сәйкестігін бастапқы тексеру жүргізеді (әрі қарай – Реттегіштің құқықтық актісі)¹⁰.
54. Қашықтықтың бірдейлікті бастапқы тексеру Куәландырушы орталықтағы ЭЦҚ жабық кілттерімен жұмыс істеу сұрақтары бойынша құқықтық актілердің қолданылатын талаптарына сәйкес жүргізіледі (әрі қарай – бұлтты ЭЦҚ ережелері)¹¹. Атап айтқанда өтініш берушіге қосфакторлы аутентификация жүргізіледі, олардың бір факторы биометриялық аутентификация болып табылады.

4 бөлім. ТІРКЕУ КУӘЛІКТЕРІНІҢ ӨМІРЛІК ЦИКЛДЕРІНЕ ҚОЙЫЛАТЫН ОПЕРАЦИЯЛЫҚ ТАЛАПТАР

4.1 параграф. ТІРКЕУ КУӘЛІКТЕРІН ШЫҒАРУҒА ӨТІНІШ

55. Куәландырушы орталықтың жазылушысының тіркеу куәлігін шығаруға өтініштері мен электрондық өтінімдерін ресімдеу принциптері Тіркеу куәліктері саясатының 4.1-параграфында анықталған.
56. Тіркеу куәлігін шығаруға өтініштер мен электрондық өтінімдер қабылданады:
 - 1) заңды тұлғалардың уәкілетті өкілдерінен;
 - 2) өз бетінше әрекет ететін жеке тұлғалардан.

4.2 параграф. ТІРКЕУ КУӘЛІКТЕРІН ШЫҒАРУҒА ӨТІНІШТЕРДІ ӨНДЕУ

57. Тіркеу куәлігін шығаруға өтініштер мен электрондық өтінімдер қолданылатын жағдайларда бұлтты ЭЦҚ Ережелерінің талаптарын ескере отырып, Реттегіштің құқықтық актісіне сәйкес өңделеді.
58. Өтінішті тіркеу (электрондық өтінімді сақтау) алдында өтініш берушіні сәйкестендіру және аутентификация жүргізіледі.
59. Өтініш тіркелгеннен кейін бас тартылады (электрондық өтінім сақталмайды), егер:
 - 1) өтініш иесі Реттегіштің құқықтық актісіне сәйкес ақпаратты түгел көрсетпеген болса;
 - 2) өтініш иесі онда жалған мәліметтер көрсеткен болса;
 - 3) тіркеу орталығына немесе Куәландыру орталығына әлеуетті жазылушының атына соттың тіркеу куәлігін беруге тыйым салатын шешімі туралы белгілі болса;
 - 4) әлеуетті жазылушы он алты жасқа толмаған болса;

¹⁰ Ережелер бекітілген күні Қазақстан Республикасы Инвестициялар мен даму министрлігінің 2015 жылғы 23 желтоқсандағы 1231 бұйрығымен бекітілген Қазақстан Республикасының негізгі куәландырушы орталығын, мемлекеттік органдардың куәландырушы орталығын, Қазақстан Республикасының ұлттық куәландырушы орталығын және Қазақстан Республикасының сенім білдірілген үшінші тарапын қоспағанда, куәландырушы орталықтың тіркеу куәліктерін беру, сақтау, кері қайтарып алу және электрондық цифрлық қолтаңбаның ашық кілтінің тиесілілігі мен жарамдылығын растау қағидалары қолданыста болды.

¹¹ Ережелер бекітілген күні Қазақстан Республикасы Цифрлық даму, инновация және аэроғарыш өнеркәсібі министрлігінің 2020 жылғы 27 қазандағы №405/НҚ бұйрығымен бекітілген Куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін жасау, пайдалану және сақтау қағидалары қолданыста болды.

-
-
- 5) Қазақстан Республикасының заңдары белгілеген өзге жағдайларда;
 - б) өтініш иесінде Куәландырушы орталық сервистерімен сәйкесетін ЭЦҚ.
60. Қазақстан Республикасының заңнамасында анықталған тіркеу куәлігін беруден бас тарту үшін негіздердің тізбесі өзгерген жағдайда, заңнаманың талаптары қолданылады. Куәландырушы орталық қызметінің ережелері заңнамада белгіленген тәртіпте сәйкестікке келтірілуге жатады.
 61. Тіркеу куәліктерін шығаруға өтініштерді (электрондық өтінімдерді) Тіркеу орталығы мен Куәландырушы орталық өтініш тіркелген (электрондық өтінім сақталған) күннен бастап 5 (бес) жұмыс күнінен аспайтын мерзім ішінде қаралады.

4.3 параграф. ТІРКЕУ КУӘЛІКТЕРІН ШЫҒАРУ

62. Куәландырушы орталықтың жазылушысына тіркеу куәлігін шығарудың принциптері мен негізгі кезеңдері Тіркеу куәліктері саясатының 4.3-параграфында анықталған.
63. Әрбір тіркеу куәлігін Куәландырушы орталық немесе тіркеу орталығында тіркеу куәлігін шығаруға жеке өтінішті тіркеу фактісі бойынша, немесе өтініш берушімен өзара әрекет жасау үшін тіркеу куәлігі қажет Банкінің ақпараттық жүйесінде тіркеу куәлігін шығаруға электрондық өтінімді сақтау фактісі бойынша жасайды.
64. Жазылушының кілттер жұбын тіркеу орталығы жағында оны шығару кезінде қорғау кілттік ақпараттың қорғалған тасымалдаушысын пайдалану есебінен, ал Куәландырушы орталық жағында – аппараттық криптографиялық модульдерді (HSM) пайдалану есебінен мүмкін болады.
65. Егер тіркеу куәлігі иесінің (жазылушының) жабық криптографиялық кілттері тіркеу орталығында жасалатын болса, онда бұл процедура, әдетте, оларды көшіру мүмкіндігіне жол бермейтін тікелей негізгі ақпараттың қорғалған тасымалдағышына орындалады. Тіркеу куәлігін шығару процедурасы аяқталғаннан кейін тіркеу орталығының қызметкері жабық криптографиялық кілттері және Куәландырушы орталықтың тіркеу куәліктері бар қорғалған негізгі тасымалдағышты өтініш берушінің қолына тапсырады.
66. Егер тіркеу куәлігі иесінің (жазылушының) жабық криптографиялық кілттері Куәландырушы орталықта шығарылған болса, онда бұл процедура Бұлтты ЭЦҚ ережелеріне сәйкес Куәландырушы орталықтың HSM-де орындалады.
67. Тіркеу орталығынан Куәландырушы орталыққа жеткізу қажет болған жағдайды жазылушының ашық кілтін уыстырып жіберуден немесе бұрмалаудан қорғауға ЭЦҚ механизімін пайдалану есебінен қол жетеді. Жазылушының ашық кілті тіркеу куәлігін шығаруға сұраныс мәнмәтініне енгізіледі, ол PKCS#10 форматында жасалады және жазылушының жабық кілтімен қол қойылады.
68. Қажет болған жағдайда Куәландырушы орталыққа жабық криптографиялық кілтті жазылушының иелену фактісін дәлелдеу тәсілі қызметін PKCS#10 форматындағы электрондық сұрау салудағы ЭЦҚ-ны тексеру болып табылады, оны сұранысты өңдеу кезінде Куәландырушы орталық атқарады.
69. Егер тіркеу куәлігін шығару өтініш бойынша қағаз тасымалдағышта жүзеге асырылса, онда Куәландырушы орталықтың жазылушысы өзінің тіркеу куәлігін тіркеу орталығына өзінің келуі барысында алады. Егер тіркеу куәлігін шығару қашықтықтан жүзеге асырылса, онда жазылушы мүдделі болған жағдайда Куәландырушы орталықтан тіркеу куәлігін қосымша сұрауы керек болады.

4.4 параграф. ТІРКЕУ КУӘЛІКТЕРІН ҚАБЫЛДАУ

70. Егер жазылушы тіркеу куәлігін шығарғаннан кейін 14 күнтізбелік күн ішінде тіркеу орталығына осы тіркеу куәлігін кері қайтарып алу туралы жазбаша өтінішпен (қағаз

тасымалдаушыдағы) жүгінбесе немесе көрсетілген кері қайтарып алуға өтініш бергенге дейін тиісті жабық кілтті пайдалана бастаса, онда тіркеу куәлігін автоматты түрде жазылушы қабылдады деп саналады.

4.5 параграф. КІЛТ ЖҰПТАРЫ МЕН ТІРКЕУ КУӘЛІКТЕРІН ПАЙДАЛАНУ

71. Криптографиялық кілттер мен тіркеу куәліктерін пайдаланудың негізгі талаптары Тіркеу куәліктерінің саясаты деп аталатын 4.5 параграфта анықталған.
72. Пайдаланар алдында тіркеу куәлігінің иесі (жазылушы) тиісті тіркеу куәлігіндегі “keyUsage” және “extendedKeyUsage” кеңейтілімдерінің мазмұнына сәйкес жабық криптографиялық кілтті таңдайды.
73. ЭЦҚ кілтке тексеру жүргізу үшін тіркеу куәлігін пайдаланушы (сенім білдіретін тұлға) реттегіштің Құқықтық актісімен регламенттелген процедураны орындайды, ол үшін атап айтқанда:
 - 1) ЭЦҚ қалыптастырылған субъектінің анықтауға мүмкіндік беретін тіркеу куәліктерінің тізбегін анықтайды және тексереді. Тіркеу куәліктерінің тізбегін тексеру барасында RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” (X.509 форматындағы ашық кілттер интернет инфрақұрылымының сертификаттарының және кері қайтарылып алынған сертификаттардың тізімінің профилі) кеңестерінде мазмұндалған алгоритм пайдаланылады.
 - 2) әр тіркеу куәлігін тексеру барысында тізбектер “keyUsage” және “extendedKeyUsage” кеңейтілімдері мазмұнының пайдалану мақсатына сәйкесетінін қосымша бақылайды.
 - 3) қол қойған тұлғада электрондық құжатқа қол қою үшін жеткілікті уәкілеттіктердің болуын өз бетінше тексереді. Куәландырушы орталықтың ақпараттық жүйесі жазылушының уәкілеттіктерін бақылау сервистерін ұсынбайды.
74. Егер тексерудің кез келген қадамы теріс нәтиже берсе немесе оны орындау мүмкін болмаса, онда сенім білдіруші тарап ЭЦҚ жарамсыз деп санайды және электрондық құжатты қабылдамайды.
75. Егер электрондық құжатта куәландырушы орталық қалыптастырған уақытты белгілеу бар болса, онда уақыт белгілеуге сенімді талап ететін әрекеттерді орындау үшін сенім білдіруші тарап та электрондық құжаттағы ЭЦҚ тексеруге ұқсас тәртіпте осы УАҚЫТ БЕЛГІЛЕРІді тексереді.
76. Егер тізбектегі тіркеу куәліктерінің кез келгені ЭЦҚ-ны тексеру сәтінде «кері қайтарып алынды» мәртебесіне ие болса, тек сенім білдіруші тарап тізбектегі тіркеу куәліктерінің бірі кері қайтарылып алынғанға дейін жазылушы қалыптастырған электрондық құжатқа сенімінің ақталатынын немесе оған сенуге болмайтынын шешу тәуекелін өз мойнына алады. Куәландырушы орталық мұндай жағдайларда тіркеу куәліктерін пайдаланушылар (сенім білдіруші тараптар) алдында жауап бермейді, себебі тіркеу куәлігін кері қайтарып алуға өтініш беру тіркеу куәлігінің нақты иесінің (жазылушының) міндеті болып табылады.
77. Егер жағдай электрондық құжат авторлары тарапынан қосымша кепілдіктердің қажеттілігін көрсетсе, онда тіркеу куәлігін пайдаланушы (сенім білдіруші тарап) тіркеу куәліктерінің иелерінен (жазылушылардан) тіркеу куәлігіне сенімді талап ететін іс-қимылдарды орындағанға дейін және Куәландырушы орталыққа жүгінбей-ақ осындай қосымша кепілдіктерді өз бетінше алады.

4.6 параграф. ТІРКЕУ КУӘЛІКТЕРІНДЕГІ ҚОЛДАНУ МЕРЗІМІН ЖАҢАЛАУ

78. Тіркеу куәліктеріндегі қолдану мерзімін жаңарту бойынша қызметті Куәландырушы орталық көрсетпейді.

4.7 параграф. ТІРКЕУ КУӘЛІКТЕРІНДЕГІ КРИПТОГРАФИЯЛЫҚ КІЛТТЕРДІ АУЫСТЫРУ

79. Тіркеу куәліктеріндегі кілттерді ауыстыру бойынша қызметті Куәландырушы орталық көрсетпейді.
80. Криптографиялық кілттерді ауыстыру үшін жазылушы Ережелердің 4.1, 4.2 және 4.3 параграфтарында анықталған тәртіпте (жаңа) тіркеу куәліктерін шығару процедурасын қайтадан өтуі тиіс.
81. Егер бұл ретте жаңа тіркеу куәлігі жабық криптографиялық кілттің әшкереленгеніне байланысты сұратылса, онда жазылушы алдымен әшкереленген тіркеу куәлігін кері қайтарып алуға өтініш, содан соң жаңадан шығаруға өтініш береді.

4.8 параграф. ТІРКЕУ КУӘЛІКТЕРІНДЕГІ ДЕРЕКТЕРДІ ӨЗГЕРТУ

82. Тіркеу куәліктеріндегі деректерді өзгерту бойынша қызметті Куәландырушы орталық көрсетпейді.
83. Тіркеу куәліктеріндегі деректерді өзгерту үшін жазылушы Ережелердің 4.1, 4.2 және 4.3 параграфтарында анықталған тәртіпте (жаңа) тіркеу куәліктерін шығару процедурасын қайтадан өтуі тиіс.
84. Бұл ретте жазылушы бірінші қолданыстағы тіркеу куәлігін кері қайтарып алуға өтініш береді, сонан соң жаңадан шығаруға өтініш береді.

4.9 параграф. ТІРКЕУ КУӘЛІКТЕРІН КЕРІ ҚАЙТАРЫП АЛУ

85. Кері қайтарып алудың ықтимал себептері келесі тізіммен анықталады:
- 1) тіркеу куәлігі иесінің (жазылушының) немесе оның өкілінің құжаттық талабы;
 - 2) тіркеу куәлігін алған кезде дұрыс емес мәліметтерді немесе құжаттардың толық емес пакетін тапсыру фактісінің анықталуы;
 - 3) тіркеу куәлігі иесінің (жазылушының) қайтыс болуы;
 - 4) тіркеу куәлігі иесінің тегінің, атының немесе әкесінің атының өзгеруі (егер жеке басын растайтын куәлікте ол көрсетілген болса);
 - 5) заңды тұлғаны – тіркеу куәлігі иесінің атауын өзгерту, қайта ұйымдастыру, тарату, заңды тұлғаның басшысын ауыстыру;
 - 6) заңды күшіне енген сот шешімі¹²;
 - 7) Тіркеу куәліктері саясатында қарастырылған басқа себептер:
 - жазылушының Банкінің ақпараттық жүйелері мен сол үшін қажетті тіркеу куәліктерін пайдаланудан өз еркімен бас тартуы;
 - Банкіде тіркеу куәліктеріне сәйкесетін жабық криптографиялық кілттердің әшкереленуіне негізі бар күмән болуы;

¹² Осы тармақтың 3-6 тармақшаларында тізіліп аталған жағдайларда тіркеу куәлігін кері қайтарып алуға негіз негіздердің болуын растайтын уәкілетті инстанцияның ресми құжатының түпнұсқасын (мысалы, қайтыс болу туралы куәлік, заңды тұлғаны қайта тіркеу туралы анықтама, сот шешімі және т.б.) ұсына отырып, жазбаша өтініш (қағаз тасымалдаушыда) беру болып табылады. Куәландырушы орталық және тіркеу орталықтары тиісті түрдегі мәліметтер көрсетілетін ақпараттық ресурстарға мониторинг жүргізбейді.

-
-
- тіркеу куәлігі иесінің (жазылушының) қолданыстағы шарттың міндеттемелерін, растамаларын және кепілдіктерін бұзғаны туралы дәлелдердің болуы;
 - жазылушының тиісті жабық кілтті иеленуі мен пайдалануының қажетті шарты болып табылатын Шарт күштің жоғалуы;
 - Реттегіштің құқықтық актісінің процедураларын, Тіркеу куәліктері саясатын, Ережелерді елеулі түрде бұза отырып, сәйкестендірілмеген немесе қате сәйкестендірілген тұлғаға тіркеу куәлігін шығаруға дәлелдердің болуы;
 - тіркеу куәліктерін шығаруға өтініштегі мәліметтің қателігіне дәлелдердің болуы;
 - тіркеу куәліктерін шығаруға өтініштегі (электрондық өтінімдегі) деректердің өзектілігін жоғалтуы;
 - сертификатты пайдалануды жалғастыру Банкінің ақпараттық жүйесі үшін қауіпті.
86. Қазақстан Республикасының заңнамасында белгіленген тіркеу куәлігін кері қайтарып алу үшін негіздемелер тізбесі өзгерген жағдайда заңнама талаптары қолданылады. Куәландырушы орталық қызметінің ережелері заңнамада белгіленген тәртіпке сәйкестікке келтіруге жатады.
87. Тіркеу орталықтары мен Куәландырушы орталық келесі тұлға арқылы ресімделген тіркеу куәлігін кері қайтарып алуға өтінішті өңдейді:
- 1) тіркеу куәліктерінің иелері;
 - 2) тіркеу куәлігі иесінің уәкілетті өкілдері болып табылатын жеке тұлғалар;
 - 3) тіркеу орталығының қызметкері.
88. Тіркеу куәлігін кері қайтарып алар алдында тіркеу орталығы және/немесе Куәландырушы орталық Өтініш берушінің сәйкестендіруімен қоса алғанда, бастамашының кері қайтарып алуға уәкілеттігін тексереді. Бұл ретте Ережелердің 3.2-параграфында көрсетілген сәйкестендіру механизмі қолданылады.
89. Тіркеу куәлігін кері қайтарып алу процедурасы Реттегіштің құқықтық актісіне сәйкес жүзеге асырылады. Өтініш негізді болған жағдайда, тіркеу куәлігі тіркеу куәлігін кері қайтарып алуға өтініш (электрондық өтінім) түскен күннен соңғы келесі жұмыс күнінен кешіктірілмей кері қайтарып алынады.
90. Сенім білдіретін тараптар өз әрекеттерінде сүйенетін барлық тіркеу куәліктерінің мәртебелерін тексереді.
91. Сенім білдіретін тараптардың тіркеу куәліктерінің мәртебелерін тексерудің үздіксіз мүмкіндігін қамтамасыз ету үшін Куәландырушы орталық:
- 1) кері қайтарып алынған тіркеу куәліктерінің жаңартылған тізімін жариялайды (<https://alfabank.kz/pki/#KRSSOS>);
 - 2) OSCP хаттамасы қызметінің жұмыс істеуін қамтамасыз етеді.
92. Тіркеу куәліктерінің қолданылуын уақытша тоқтата тұру немесе қолданылуын жаңғырту бойынша қызметтерді Куәландырушы орталық көрсетпейді.
93. Тіркеу куәлігі иесінің (жазылушының) жабық кілтін депозиттеу бойынша қызметті¹³ Куәландырушы орталық көрсетпейді.

¹³ Депозиттеу – Ережелер мәнмәтінінде, – тиісті тіркеу куәлігі иесінің бастамасы бойынша Куәландырушы орталықта жабық криптографиялық кілттердің резервтік көшірмелерін уақытша сақтау. Тіркеу куәлігі иелерінің өзінің жабық криптографиялық кілттерін Бұлтты ЭЦҚ ережелеріне сәйкес Куәландырушы орталықтың ашық кілттер инфрақұрылымында тұрақты сақтауы және пайдалануы «депозиттеу» түсінігіне жатпайды.

5 бөлім. ФИЗИКАЛЫҚ, ОПЕРАЦИЯЛЫҚ ЖӘНЕ БАСҚАРУШЫ БАҚЫЛАУЛАР

5.1 параграф. ФИЗИКАЛЫҚ БАҚЫЛАУ

94. Куәландырушы орталықты физикалық бақылаудың егжей-тегжейлі шаралары Банкінің ішкі құжаттарында анықталған және бекітілген және олар Ережелерде ашылмайды. Осы бөлімде аталған шараларға жалпы шолу келтірілген.
95. Куәландырушы орталықтың Ақпараттық жүйесі төтенше оқиға болған жағдайда резервтеу және жұмыс істеуін қалпына келтіру мақсатында әртүрлі объектілерде орналасқан деректерді өңдейтін екі орталықпен (негізгі және резервтік) қамтамасыз етілген.
96. Негізгі және дата орталыққа физикалық қол жеткізу ұйымдастырылған және бірдей қауіпсіздік шараларымен бақыланады.
97. Серверлік жайлар жүйелермен жабдықталған:
 - 1) қол жетімділікті бақылау және басқару;
 - 2) күзет сигнализациясы;
 - 3) бейнебақылау;
 - 4) кепілді электрооректендіру;
 - 5) электрлік жерге тұйықтау;
 - 6) микроклиматты қамтамасыз ету;
 - 7) өрт сигнализациясы;
 - 8) газбен автоматты өрт сөндіру.

5.2 параграф. ОПЕРАЦИЯЛЫҚ БАҚЫЛАУ

98. Куәландырушы орталықтың Деректерді өңдеу орталығы 24/7/365 режимінде тәулік бойы техникалық қолдаумен қамтамасыз етілді, оған құрал-жабдықты қайта жүктеу мен жинақтаушыларды ауыстыру кіреді.
99. Қызмет көрсету деңгейі туралы келісім бойынша деректерді өңдеу орталықтарында құрал-жабдықтың және байланыс арналарының жұмыс істемей қалуы себебінен құрал-жабдықтың тұрып қалуы жаңғырту бойынша жоспарлы жұмыстардан немесе қызмет жеткізушіге бағынбайтын форс-мажорлық жағдайлардан өзге жылына 18 сағаттан (99.8%) аспайды.
100. Деректерді өңдеу орталықтарына қызмет жеткізушінің назар аудару уақыты – Куәландырушы орталық өтінімді рәсімдеген сәттен бастап 1 сағаттан артық емес.
101. Куәландырушы орталықтың жұмысшы процедуралардың бүкіл жиынынан ерекше ұйымдастыру шараларымен аппараттық криптографиялық модульдерді (Hardware Security Module, HSM) және олардың негізгі материалдарын баптау және қызмет көрсету процедурасы ерекшеленіп бөлінген.
102. HSM құрылғысына HSM-ге және кілттерге физикалық қол жеткізуге арналған криптографиялық кілттер енгізілген сәттен бастап кем дегенде Банкінің еік уәкілетті қызметкерінің қатысуы қажет болады.
103. HSM-ге қол жеткізуді және оның жұмыс қабілеттілігін бақылауды жүзеге асыратын қызметкерлер Куәландырушы орталықтың криптографиялық кілттерімен жұмыс істемейді және кересінше.

5.3 параграф. ҚЫЗМЕТКЕРЛЕРДІ БАҚЫЛАУ

104. Куәландырушы орталықта және тіркеу орталықтарында лауазымдарға тағайындағандар алдында ізденушілер Қазақстан Республикасының Еңбек кодексінде анықталған

құжаттарды тапсырады және қызметкерлерді іріктеу жөніндегі Банкінің ішкі құжатына сәйкес скринингтен өтеді¹⁴.

105. Куәландырушы орталықтың мамандары мен басшылары үш жылда бір реттен сиретпей оқытудан немесе сертификаттаудан өтеді.
106. Куәландырушы орталық қызметкерлерінің қызметтік ақпаратқа рұқсатсыз қол жеткізгені және ақпараттық қауіпсіздік талаптарын өзге бұзғаны үшін жауапкершілігі еңбек шартында және лауазымдық нұсқаулықтарда қарасырылған.
107. Ақпараттық қауіпсіздік талаптарын бұзу фактісі бойынша тәртіптік жазалар жұмыс берушінің ішкі құжатына сәйкес бұйрықтармен тағайындалады және шығарылады¹⁵.
108. Куәландырушы орталықтың және тіркеу орталықтары қызметкерлерінің лауазымдық міндеттерін құзыретті орындауы үшін қажетті Банкінің ішкі нормативтік құжаттарының құқықтық актілерінің мәтіндеріне қол жеткізу Банкінің ішкі ақпараттық ресурсы арқылы беріледі.

5.4 параграф. БАҚЫЛАУ ХАТТАМАЛАУЫНЫҢ ПРОЦЕДУРАЛАРЫ

109. Хаттамалауға жататын оқиғалар типтері Тіркеу куәліктері саясатының 5.4 параграфында анықталған.
110. Бақылау хаттамасы жазбасының құрылымына кіреді:
 - 1) жазба күні мен уақыты;
 - 2) жазбаның реттік нөмірі;
 - 3) хаттамалауға жататын оқиғаны бастамалаған мәннің біртектілігі;
 - 4) оқиға типі;
 - 5) жазба көзі.
111. Куәландырушы орталықтың ақпараттық жүйесінің бақылау хаттамалары үздіксіз жүргізіледі, Қағидалардың 5.5 параграфына сәйкес тәулік сайын резервтік көшіруге, ай сайын архивтеуге және архивке өткізуге жатады, архивте регламенттелген мерзім ішінде сақталады.
112. Машиналық тасымалдаушыға жазар алдында Куәландырушы орталықтың ақпараттық жүйесінің бақылау хаттамаларының архивтік көшірмесі шифрленеді және хэш-кодпен жабдықталады.
113. Тіркеу куәліктері иелерінің (жазылушылардың) және Куәландырушы орталық контрагенттерінің құжаттық материалдары іс жүргізу сұрақтары бойынша Банкінің ішкі құжаттарына сәйкес тіркеледі, жүйеленеді және сақталады¹⁶.

5.5 параграф. АРХИВ ЖҮРГІЗУ

114. Куәландырушы орталық архив жүргізеді, онда Тіркеу куәліктері саясатының 5.5 параграфында анықталған жазбаша және электрондық құжаттар сақталады.
115. Архив ақпаратын тасымалдаушыларды сақтау, ақпараттың архивтік тасымалдаушыларын таңбалау, архив деректерін рұқсатсыз көруден, өзгертуден және алып тастаудан қорғау ақпараттық жүйе деректерін резервтеу бойынша Банкінің ішкі құжаттарына сәйкес жүзеге асырылады¹⁷.

¹⁴ Ережелер бекітілген күні 2020 жылғы 18 ақпандағы Банк Басқармасының №12 хаттамалық шешімімен бекітілген Қызметкерлер іріктеу жөніндегі нұсқаулық қолданыста болды.

¹⁵ Ережелер бекітілген күні 2015 жылғы 30 желтоқсандағы Банк Басқармасының №80 шешімімен бекітілген Тәртіптік жаза қолдану туралы қағида қолданыста болды.

¹⁶ Ережелер бекітілген күні 2020 жылғы 28 қаңтардағы Банк Басқармасының №7 қаулысымен бекітілген Іс жүргізуді ұйымдастыру ережесі қолданыста болды.

¹⁷ Ережелер бекітілген күні 2015 жылғы 14 қазандағы Банк Басқармасының №59 хаттамалық шешімімен бекітілген

-
-
116. Куәландырушы орталықтың құпия деректерін тасымалдаушыны кәдеге жарату Деректерді жою сұрақтары бойынша Банкінің ішкі құжаттарына сәйкес жүзеге асырылады¹⁸.

5.6 параграф. КУӘЛАНДЫРУШЫ ОРТАЛЫҚТЫҢ КРИПТОГРАФИЯЛЫҚ КІЛТТЕРІН АУЫСТЫРУ

117. Криптографиялық кілттерді ауыстыру Куәландырушы орталықтың аппараттық криптографиялық модульдерімен (HSM) жұмыс сұрақтары бойынша Банкінің ішкі құжаттарына сәйкес жүзеге асырылады¹⁹.

5.7 параграф. ТӨТЕНШЕ ОҚИҒАЛАР НЕМЕСЕ ӘШКЕРЕ БОЛУ ЖАҒДАЙЫНДА ЖҰМЫС ІСТЕУДІ ҚАЛПЫНА КЕЛТІРУ

118. Куәландырушы орталық сервистерінің жұмыс істеуінің үзілуіне әкеп соғатын төтенше оқиғалар жағдайында Жұмыс істеуді қалпына келтіру жоспарын қолданысқа енгізу туралы шешім қабылданады.
119. Куәландырушы орталықтың Жұмыс істеуді қалпына келтіру жоспарында қарастырылған:
- 1) деректерді өңдейтін негізгі немесе резервтік орталықтар базасында қалпына келтіру алаңын таңдау;
 - 2) резервтік немесе архивтік көшірмелерден жұмысшы жазбаларын қалпына келтіру.
120. Деректерді өңдейтін резервтік орталық қосалқы құрал-жабдықпен қамтамасыз етілген. Куәландырушы орталықтың жұмысшы жазбаларының резервтік және архивтік көшірмелерін жасау және сақтау, сонымен қатар Жұмыс істеуді қалпына келтіру жоспарының нысаны ақпараттық жүйе деректерін резервтеу бойынша Банкінің ішкі құжатымен регламенттелген²⁰.
121. Куәландырушы орталықтың есептеу, бағдарламалық ресурстарының және/немесе ақпараттық жүйесі деректерінің бүліну жағдайлары Куәландырушы орталық қызметкерлерінің штаттан тыс және дағдарыс жағдайларындағы іс-әрекеті тәртібін белгілейтін Банкінің ішкі құжатымен регламенттелген тәртіпте өңделеді²¹.
122. Куәландырушы орталық Куәландырушы орталықтың криптографиялық кілттерінің тіркеу куәлігін кері қайтарып алу туралы шешім қабылдаған жағдайда келесі процедуралар орындалады:
- 1) Куәландырушы орталық Қазақстан Республикасының Негізгі куәландырушы орталығы (әрі қарай – ҚР НТО) кері қайтарып алған тіркеу куәліктерінің ағымдағы тізімін сақтайды.
 - 2) Куәландырушы орталық ҚР НТО-ға тіркеу куәлігін (куәліктерін) кері қайтарып алу туралы өтінішпен жүгінеді және Интернет желісіндегі Банкінің ресми ақпарат ресурсындағы өз тарауында кері қайтарып алу туралы ақпаратты жариялайды.

Ақпараттық жүйе деректерін резервтеу ережелері қолданыста болды.

¹⁸ Ережелер бекітілген күні 2019 жылғы 9 шілдедегі Банк Басқармасының №46 хаттамалық шешімімен бекітілген Электрондық тасымалдаушылардағы ақпаратты жою ережелері қолданыста болды.

¹⁹ Ережелер бекітілген күні Куәландырушы орталықтың HSM модульдерімен жұмыс жөніндегі жеке нұсқаулық әзірлену үстінде болды.

²⁰ Ережелер бекітілген күні 2015 жылғы 14 қазандағы Банк Басқармасының №59 хаттамалық шешімімен бекітілген Ақпараттық жүйе деректерін резервтеу ережелері қолданыста болды.

²¹ Ережелер бекітілген күні 2021 жылғы 15 маусымдағы Банк Басқармасының №37 хаттамалық шешімімен бекітілген Куәландырушы орталық қызметкерлерінің штаттан тыс және дағдарыс жағдайларындағы іс-әрекеті тәртібі туралы нұсқаулық қолданыста болды.

-
-
- 3) Жұмыс істеуді қалпына келтіру жоспарына сәйкес тіркеу куәліктерін пайдаланушыларға (сенім білдіруші тарап) КО тіркеу куәліктерін кері қайтарып алу туралы қосымша хабарлауға арналған өзге де орынды шараларды қолданады.
 - 4) Куәландырушы орталық қызметін тоқтату жағдайын өзге 6.1 параграфқа сәйкес жаңа криптографиялық кілттер генерацияланады.
123. Жұмыс істеуді қалпына келтіру жоспарының өзектілігі Куәландырушы орталықтың ақпараттық жүйесіне өзгерістер енгізілуіне қарай немесе Куәландырушы орталықтың ақпараттық жүйесін негізгі және резервтік деректерді өңдеу орталықтары арасында қайта қосу нәтижелері бойынша, бірақ жылына бір реттен сиретпей тексеріледі.

5.8 параграф. КУӘЛАНДЫРУШЫ ОРТАЛЫҚ ЖҰМЫСЫНЫҢ ТОҚТАУЫ

124. Куәландырушы орталық жұмысын тоқтау туралы шешім қабылданған жағдайда Банк контрагенттерін, оның ішінде тіркеу куәліктерінің иелері мен пайдаланушыларымен (Куәландырушы орталықтың және сенім білдіруші тараптың жазылушыларымен) қоса, Куәландырушы орталықтың жазбаларын беру және архивтік сақтау Қазақстан Республикасының «Электрондық құжат және электрондық цифрлік қолтаңба туралы» Заңына (22 бап) сәйкес ұйымдастырылады.

6 бөлім. ҚАУІПСІЗДІКТІ ТЕХНИКАЛЫҚ БАҚЫЛАУ

6.1 параграф. КРИПТОГРАФИЯЛЫҚ КІЛТТЕРДІ

ГЕНЕРАЦИЯЛАУ ЖӘНЕ ОРНАТУ

125. Куәландырушы орталықтың криптографиялық кілттерін генерациялаудың әрбір фактісі бойынша хаттама жасалады, оған күні қойылады және процедураға қатысқан тұлғалар қол қояды. Хаттамалар Банкінің іс жүргізуді ұйымдастыру ережелеріне сәйкес сақталады²².
126. Куәландырушы орталық қызметкерлерінің немесе ақпарат жүйесінің жазылушылардың криптографиялық кілттерге қол жеткізуіне тек кілттік ақпараттың қорғалған тасымалдағыштарын немесе арнайы қолданбалы бағдарламалық жасақтаманы және Бұлтты ЭЦҚ ережелеріне сәйкес тіркеу куәліктері иелерінің жабық кілттерімен жұмысқа (жасау, сақтау және пайдалану) арналған жекелеген аппараттық криптографиялық модульдерді (HSM) пайдалану арқылы жол берілмейді.
127. Тек ерекше жағдайларда, Куәландырушы орталықтың ақпараттық жүйесінің технологиялық жабық кілтін қорғалған негізгі ақпарат тасымалдаушысынан тікелей пайдалануға техникалық мүмкіндік болмаған кезде, мұндай жабық технологиялық кілтті пайдалануға активтеу деректерін міндетті түрде пайдалана отырып, негізгі ақпаратты еркін тасымалдағышқа сақтау генерацияланғаннан кейін жол беріледі.
128. Куәландырушы орталық пен оның жазылушыларының ашық криптографиялық кілттерінің біртұтастығы мен тиесілілігі оларды генерациялағаннан бастап тіркеу куәліктерін шығарғанға дейінгі кезеңде ЭЦҚ механизмімен қорғалады. Ашық кілттер жазылушылардан Куәландырушы орталыққа тек PKCS#10 форматы негізінде электрондық құжаттар нысанында беріледі.
129. Куәландырушы орталықтың ашық криптографиялық кілттері сенім білдіруші тараптарға тіркеу куәліктері нысанында беріледі.

²² Ережелер бекітілген күні 2020 жылғы 28 қаңтардағы Банк Басқармасының №7 қаулысымен бекітілген Іс жүргізуді ұйымдастыру ережелері қолданыста болды.

-
-
130. Куәландырушы орталықтың жазылушылары Куәландырушы орталықтың ашық криптографиялық кілттерін тіркеу орталығында қолдан қолға, жеке немесе өзінің тіркеу куәлігіне тізбектің бір бөлігі ретінде сұрай алады.
 131. Куәландырушы орталықтың ашық криптографиялық кілттері (тіркеу куәліктерінің құрамында) сонымен қатар <https://alfabank.kz/pki/#KRSSOS> адресі бойынша Банкінің ресми ақпараттық ресурсынан жүктеп алу үшін қол жетімді.
 132. Куәландырушы орталық төмендегі құжаттарға сәйкес пайдалануға арналған криптографиялық кілттерді тіркейді:
 - 1) МЕМСТ 34.310-2004 (ЭЦҚ) халықаралық стандартына.
Жабық кілттің ұзындығы – 256 қосарлы разряд;
Ашық кілттің ұзындығы – 512 қосарлы разряд;
 - 2) ҚРС#1 (RFC 8017) халықаралық кеңестеріне.
Жабық кілттің ұзындығы – 2048 қосарлы разрядтан кем емес.
Ашық кілттің ұзындығы – 2048 қосарлы разрядтан кем емес.

6.2 параграф. ЖАБЫҚ КРИПТОГРАФИЯЛЫҚ КІЛТТЕРДІ ҚОРҒАУ ЖӘНЕ КРИПТОГРАФИЯЛЫҚ МОДУЛЬДЕРДІ ИНЖЕНЕРЛІК БАҚЫЛАУ

133. Куәландырушы орталықтың жабық криптографиялық кілттерін генерациялау тікелей осы кілттер алғаш рет пайдаланылған аппараттық криптографиялық модульде (HSM) іске асырылады. Қайтадан генерацияланған жабық кілттерді қосымша активтеу қажет емес.
134. Тіркеу куәліктері саясатының талаптарына сәйкес Куәландырушы орталықтың жабық криптографиялық кілттері жасалғаннан кейін депозиттелмейді. Сонымен қатар, куәландырушы орталықтың жұмысындағы төтенше оқиғадан немесе өзге жаңылыстан кейін ақпараттық жүйенің жұмыс істеуін қалпына келтіру мүмкіндігін қамтамасыз ету мақсатында Куәландырушы орталықтың әр жаңа жабық криптографиялық кілтін генерациялағаннан кейін бірден осы сәтте пайдаланылатын Куәландырушы орталықтың жабық криптографиялық кілттерінің барлығының резервтік көшірмесін жасайды және сақтайды.
135. Резервтік көшірме жасау барысында Куәландырушы орталықтың жабық криптографиялық кілттері шифрленеді және аппараттық криптографиялық модульден (HSM) шифрленген түрде шығарылады, және Куәландырушы орталықтың жабық кілттері құрылғы ішінде шифрсіздендіріледі.
136. Куәландырушы орталықтың жабық криптографиялық кілттерінің резервтік көшірмелерін аппараттық криптографиялық модульден (HSM) шығарған кезде құпия қалыптастырылады (активтеу деректері), ол n бөліктерге бөлінеді. Резервтік көшірмеден алып қалпына келтіргеннен кейін кілттерді активтеу үшін сақтаушылары қатысқан жағдайда құпияның m бөлігін іске қосу жеткілікті. m және n параметрлерінің ағымдағы мәні HSM паспортында бегіленген²³.
137. Куәландырушы орталықтың жабық кілттерінің резервтік көшірмелерін сақтайтын орын мен құпия бөлігін сақтаушылардың лауазымдық құрамы Банкінің ішкі құжаттарында анықталады және белгіленеді.

²³ Ережелер басылып шыққан сәтте $n = 3$ және $m = 2$. Бұл талаптар тіркеу куәліктері иелерінің (жазылушылардың) жабық кілттерін өңдеуге арналған мамандандырылған HSM-ге таралмайды. Көрсетілген HSM-нен жабық кілттерді құпия бөлінген схема бойынша резервтеу (көрсетілген процедура қолданылатын жағдайда) Бұлтты ЭЦҚ ережелеріне сәйкес жүзеге асырылады.

-
-
138. Куәландырушы орталықтың ақпараттық жүйесінің үздіксіз жұмыс істеуін қамтамасыз ету мақсатында аппараттық криптографиялық модульдердегі (HSM) жабық криптографиялық кілттер оларды генерациялағаннан немесе резервтік көшірмеден қалпына келтіргеннен кейін жою (кетіру) сәтіне дейін активтелген күйінде қалады.
 139. Куәландырушы орталықтың ауыстыру немесе қолданылу мерзімінің аяқталуы салдарынан өзектілігін жоғалтқан жабық криптографиялық кілттері сертификатталған АКҚК-ның пайдалану-техникалық құжаттамасына сәйкес аппараттық криптографиялық модульдердің (HSM) штаттық қызметітерімен жойылады.
 140. Куәландырушы орталықтың ауыстыру немесе қолданылу мерзімінің аяқталуы салдарынан өзектілігін жоғалтқан жабық криптографиялық кілттерінің резервтік көшірмелері архивтік сақтауға жатпайды және деректерді жою сұрақтары бойынша Банкінің ішкі құжаттарына сәйкес жойылады²⁴.
 141. Куәландырушы орталықтың өнім ортасының қолданылу мерзімінің аяқталуы немесе бұзылғаннан кейін жөндеуге жарамау салдарынан пайдаланудан шығарылған жабық криптографиялық кілттері әлдеқандай бір кездері құрамында болған аппараттық криптографиялық модульдері (HSM) Банкіден шығаруға немесе кез келген сапада қайтадан пайдалануға, оның ішінде жекелеген түйіндер мен тетіктерге бөлшектеуге жатпайды. Баланстан есептен шығарылғаннан кейін жоғарыда көрсетілген HSM деректерді жою сұрақтары бойынша Банкінің ішкі құжаттарына сәйкес жоюға жатады¹⁸.

6.3 параграф. КРИПТОГРАФИЯЛЫҚ КІЛТТЕРДІ БАСҚАРУДЫҢ ӨЗГЕ АСПЕКТІЛЕРІ

142. Ашық кілті Куәландырушы орталық шығарған тіркеу куәлігімен куәландырылған криптографиялық кілттердің кез келген жұбын пайдалану кезеңі тіркеу куәлігінің қолданылу мерзіміне сәйкеседі, ақпаратты шифрден шығару немесе ЭЦҚ тексеру мақсатында жоғарыда сипатталған кілттер тіркеу куәлігінің қолданылу мерзімі аяқталғаннан кейін де пайдаланылатыннан өзге жағдайда.
143. Тіркеу куәліктерінің иелері мен пайдаланушылары (Куәландырушы орталықтың жазылушылары мен өнім білдіруші тараптар) қолдану мерзімі өтіп кеткеннен кейін тіркеу куәліктерін (криптографиялық кілттерді) пайдаланбайды, алдыңғы тармақта көрсетілген мақсаттардан өзге жағдайда.
144. Криптографиялық кілттерді пайдаланудың қалған аспектілері Тіркеу куәліктері саясатының 6.3 параграфында анықталған.

6.4 параграф. АКТИВТЕУ ДЕРЕКТЕРІ

145. Жабық криптографиялық кілттерді пайдалану үшін Куәландырушы орталық жазылушысының құпиясөз нысанында активтеу деректерін жасауы және қолдануы қажет.
146. Тіркеу куәлігі иесінің (Куәландырушы орталықтың жазылушысы) жабық криптографиялық кілтін активтеуге арналған құпиясөз Банкінің ішкі құжатының талаптарына сәйкес пайдаланылады²⁵.

²⁴ Ережелер бекітілген күні Банк Басқармасының №46 хаттамалық шешімімен бекітілген Электрондық тасымалдағыштаға ақпаратты жою ережелері қолданыста болды.

²⁵ 2019 жылғы 30 сәуірдегі Банк Басқармасының №27 хаттамалық шешімімен бекітілген Құпиясөздер мен аутентификация құралдарын пайдалану нұсқаулығы, 2020 жылғы 11 қыркүйектегі Банк Басқармасының №64 хаттамалық шешімімен енгізілген толықтыруларымен және өзгерістерімен бірге қолданыста болды.

-
-
147. Куәландырушы орталықтың жабық криптографиялық кілттерін активтеуге арналған құпияның бір бөлігін сақтайтын әр сақтаушы өз құпиясөзін құпия сақтайды және еңбек шарты мен лауазымдық нұсқаулығында қарастырылған осы талапты бұзғаны үшін жауапты болады.
148. Куәландырушы орталықтың жабық криптографиялық кілттерінің активтеу деректері көрсетілетін аппараттық токендер активтеу деректері өзектілігін жоғалған жағдайда қайта жазылады (нөлденеді) және сол мақсаттарда қайтадан пайдалаатын сәтке дейін немесе кейіннен міндетті түрде жойыла отырып, есептен шығарылғанға дейін құпиясөздердің резервтік көшірмелерін сақтау үшін көзделген тәртіпте сақталады. Құпияның бөліктерін сақтау үшін бұрын пайдаланылған қорғалған тасымалдағыштар Банкіден шығаруға, бөлшектеуге немесе өзге мақсаттарда қайтадан пайдалануға жатпайды

6.5 параграф. ЕСЕПТЕУ РЕСУРСТАРЫНЫҢ ҚАУІПСІЗДІГІН БАҚЫЛАУ

149. Куәландырушы орталықтың есептеу ресурстары, бағдарламалық жасақтамасы және ақпараттық жүйесінің деректері Банкінің ақпараттық қауіпсіздік саясатына сәйкес рұқсатсыз қол жеткізуден қорғалады және Ережелерде ашылмайды. Бұл шараларға жалпы шолу Тіркеу куәліктері саясатының 6.5 параграфында келтірілген.

6.6 параграф. ДАМУДЫ ЖӘНЕ ҚАУІПСІЗДІКТІ БАСҚАРУДЫ БАҚЫЛАУ

150. Куәландырушы орталық өз қызметінде пайдаланатын барлық қолданбалы бағдарламалық жасақтама лицензиялық өнім болып табылады және оның айырықша құқығы Банкіге тиесілі емес.
151. Көрсетілген бағдарламалық жасақтаманың тиісінше жұмы істеуін қамтамасыз ету бойынша міндеттемені шарт бойынша жеткізуші (сервис ұйымы) орындайды.

6.7 параграф. ЖЕЛІ ҚАУІПСІЗДІГІН БАҚЫЛАУ

152. Куәландырушы орталықтың қызметтері Банктің ішкі құжатына сәйкес рұқсатсыз қол жеткізуден және араласудан қорғалған Банкінің корпоративтік желісінде орындалады²⁶.
153. Куәландырушы орталық модульдерінің (компоненттерінің) түсіндірме жазбамен өзара әрекетінің схемасы Ережелердің 1 қосымшасында берілген.

6.8 параграф. УАҚЫТ БЕЛГІЛЕРІ

154. Тіркеу куәліктеріндегі, кері қайтарылып алынған тіркеу куәліктерінің тізімдеріндегі, OCSP түбіртектеріндегі (қызмет жауаптарындағы) күн мен уақыты туралы ақпарат ЭЦҚ-мен расталады.

7 бөлім. ТІРКЕУ КУӘЛІКТЕРІНІҢ, СОРС ЖӘНЕ OCSP ПРОФИЛЬДЕРІ

7.1 параграф. ТІРКЕУ КУӘЛІГІНІҢ ПРОФИЛЬДЕРІ

155. Куәландырушы орталық шығарған тіркеу куәліктері 3 (v.3) версиясы бойынша таңбаланған RFC 3280 кеңестеріне сәйкеседі.
156. Тіркеу куәліктеріндегі негізгі жолдар мен кеңейтілімдер олардың мазмұны мен синтаксисіне қойылатын талаптармен бірге, сонымен қатар тіркеу куәліктерінде көрсетілген криптографиялық алгоритмдер және олардың объектілік

²⁶ Ережелер бекітілген күні 2019 жылғы 14 тамыздағы Банк Басқармасының №55 хаттамалық шешімімен бекітілген Есептеу желісі қауіпсіздігін қамтамасыз ету стандарты қолданыста болды.

сәйкестендіргіштері Интернет желісіндегі Банкінің ресми ақпараттық ресурсында <https://alfabank.kz/pki/#SS> адресі бойынша жарияланған.

157. Куәландырушы орталық шығарған тіркеу куәліктерінде көрсетілетін аттар ITU-T X.520 есімдер форматына сай Ереженің 3.1 параграфінің талаптарына сәйкеседі.
158. ЭЦҚ-ны пайдалану және ЭЦҚ-ның тіркеу куәлігін қалыптастыру және пайдалану процесінде қолданылатын криптографиялық түрлендіру алгоритмдеріне бастапқы деректері (негізгі талаптары) бар ЭЦҚ тіркеу куәлігін алу схемалары Ережелердің 2 қосымшасында келтірілген.
159. Куәландырушы орталық шығарған тіркеу куәліктері қолданылатын ақпараттық жүйелерге сәйкес келетін Тіркеу куәліктері саясатының объектілік сәйкестендіргіштері Ережелердің 1.4 параграфына сәйкес белгіленеді. «CertificatePolicies» сертификаттарының кеңейтілімдері көрсетілген параграфқа сәйкес толтырылады.

7.2 параграф. КЕРІ ҚАЙТАРЫЛЫП АЛЫНҒАН ТІРКЕУ КУӘЛІКТЕРІ ТІЗІМІНІҢ ПРОФИЛЬДЕРІ

160. Куәландырушы орталық шығарған кері қайтарылып алынған тіркеу куәліктерінің тізімі 2 (v.2) версиясы бойынша таңбаланған RFC 3280 кеңестеріне сәйкеседі.
161. Кері қайтарылып алынған тіркеу куәліктерінің тізімінде берілген негізгі жолдар мен кеңейтілімдер олардың мазмұнына қойылатын талаптармен бірге Интернет желісіндегі Банкінің ресми ақпараттық ресурсында <https://alfabank.kz/pki/#SSOS> адресі бойынша жарияланған

7.3 параграф. OCSP СЕРВИСІНІҢ ПРОФИЛІ

162. Куәландырушы орталық шығарған тіркеу куәліктерінің мәртебесі туралы ақпарат алуға арналған OCSP сервисі 1 версия форматында ұсынылады (RFC 2560 “X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP”, X.509 ашық кілттер интернет инфрақұрылымының сертификаттары мәртебесінің онлайн хаттамасы кеңестеріне сәйкес).

8 бөлім. ҚЫЗМЕТТІ ТЕКСЕРУ

163. Куәландырушы орталықты аккредитациялау үш жыл²⁷ мерзімге жүзеге асырылады және ол Уәкілетті органның Құқықтық актісіне сәйкес орындалады²⁸.
164. Сонымен қатар, құрамына Куәландырушы орталықтың басқармасы кіретін Ақпараттық қауіпсіздік департаментінің қызметі Банкінің ішкі құжатына сәйкес жоспарлы негізде ішкі аудиттен өткізіледі²⁹.

9 бөлім. ӨЗГЕ СҰРАҚТАР

9.1 параграф. ТАРИФТЕР

165. Куәландырушы орталық банкінің қызмет көрсетілетін ақпараттық жүйелерінің пайдаланушыларына келесі қызметтерді көрсетеді:

²⁷ Қазақстан Республикасының «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Заңы, 20-2 бап.

²⁸ Ережелер бекітілген күні Қазақстан Республикасы Цифрлық даму, инновация және аэроғарыш өнеркәсібі министрлігінің 2020 жылғы 1 маусымдағы № 224/НҚ “Куәландырушы орталықтарға аккредитация жүргізу қағидаларын бекіту туралы» бұйрығы қолданыста болды.

²⁹ Ережелер бекітілген күні Директорлар кеңесінің 2020 жылғы 2 маусымдағы №10 хаттамалық шешімімен бекітілген «Ішкі аудит саясаты» қолданыста болды.

-
- 1) Занды және жеке тұлғалардың өтініштері бойынша жазылушыларға тіркеу куәліктерін шығару, өтініштерді тіркеумен қоса;
 - 2) тіркеу куәліктерін кері қайтарып алу;
 - 3) тіркеу куәліктері мен кері қайтарылып алынған тіркеу куәліктерінің тізімін қоймаға орналастыру, сонымен қатар Интернет желісіндегі Банкінің ресми ақпараттық ресурсында Тіркеу куәліктері саясатын, Ережені және Куәландырушы орталықтың қызметтері туралы клиентке бағдарланған өзге өзекті ақпаратты жариялау;
 - 4) OSCP хаттамасы бойынша онлайн режимде тіркеу куәліктерінің мәртебесі туралы ақпарат беру;
 - 5) TSP («уақыт белгілері» сервисі) хаттамасы бойынша онлайн режимде деректерді нақты уақытқа байластыру.
166. Куәландырушы орталықтың қызметтерін ұсынуға кеткен шығыстар куәландырушы орталықтың сервистерін пайдаланатын Банк өнімдері желісінің бағаларына енгізілген. Куәландырушы орталықтың қызметтері жеке тарифтелмейді және төленбейді

9.2 параграф. ЖАУАПКЕРШІЛІК

167. Куәландырушы орталық қызмет көрсететін ашық кілттер инфрақұрылымына қатысушылардың жауапкершілігі Қазақстан Республикасының заңнамасында белгіленген³⁰.
168. Куәландырушы орталық пен тіркеу орталықтары қызметкерлерінің жауапкершілігі еңбек шартында және лауазымдық нұсқаулықтарда белгіленген.

9.3 параграф. АҚПАРАТТЫҢ ҚҰПИЯЛЫҒЫ

169. Куәландырушы орталықтың қоймасында көпшілікке қолжетімді ақпараттан басқа, куәландырушы орталықтың қызметі туралы өзге де ақпарат Ақпаратты қорғау сұрақтары бойынша Банкінің ішкі құжатына сәйкес құпия ретінде жіктеледі³¹. Осы құжат көрсетілген ақпаратпен жұмыстың жауапкершілігі мен тәртібін регламенттейді.
170. Тіркеу куәлігін шығаруға өтініштің (электрондық өтінімнің) нысаны өтініш берушінің Қазақстан Республикасының дербес деректер және оларды қорғау сұрақтары бойынша заңнамасына сәйкес оның дербес деректерін жинауға және өңдеуге келісімін растайды³², оның ішінде Куәландырушы орталыққа өтініш берушінің тіркеу куәлігі мен қоймадағы оның мәртебесі туралы ақпаратты жариялауға рұқсат береді.

9.4 параграф. ҚАТЫСУШЫЛАРДЫҢ ДЕРБЕС ДЕРЕКТЕРІН ҚОРҒАУ

171. Куәландырушы орталық Қазақстан Республикасының дербес деректер және оларды қорғау сұрақтары бойынша заңнамасына сәйкес ашық кілттер инфрақұрылымына қатысушылардың дербес деректерінің қорғалуын қамтамасыз етеді.

9.5 параграф. ЗИЯТКЕРЛІК МЕНШІК ҚҰҚЫҒЫ

172. Куәландырушы орталық тіркеу куәліктерінің иелері мен пайдаланушыларына (жазылушылар мен сенім білдірген тараптарға) деректердің толықтығы мен тұтастығы талаптарын сақтай отырып, тіркеу куәліктерін ерекше емес тегін негізде көшіруге және таратуға тыйым салмайды.

³⁰ Қазақстан Республикасының «Әкімшілік құқық бұзушылық туралы» Кодексі, 640 бап

³¹ Ережелер бекітілген күні Банк Басқармасының 2020 жылғы 16 маусымдағы №41 хаттамалық шешімімен бекітілген «Қорғалуға жататын ақпаратпен жұмыс ережелері» қолданыста болды.

³² Қазақстан Республикасының «Дербес деректер және оларды қорғау туралы» Заңы, 8 бап.

173. Куәландырушы орталық шығарған тіркеу куәліктеріне сәйкесетін жабық криптографиялық кілт осы тіркеу куәлігі иесінің (жазылушының) меншігі болып табылады. Оған сәйкес ашық криптографиялық кілт пен тіркеу куәлігі Банкінің меншігі болып табылады.

9.6 параграф. КЕПІЛДІКТЕР ЖӘНЕ КУӘЛАНДЫРУЛАР

174. Куәландырушы орталық қамтамасыз етеді:

- 1) өзі шығарған тіркеу куәліктеріндегі деректердің тіркеу орталығы немесе Банкінің мүдделі ақпараттық жүйесі тіркеу куәлігін шығаруға сұраныстың құрамында берген мәліметтерге сәйкестігі және осы тіркеу куәліктерінде Куәландырушы орталық қызметкерлерінің қасақана немесе қателесіп жасаған әрекеттерінің нәтижесінде осы мәліметтердің кездейсоқ немесе қасақана бұрмалануының болмауы;
- 2) көрсетілетін қызметтердің келесі (тіркеу куәліктерін шығару, кері қайтарып алу, СОРС шығару, ОСП және ТСП онлайн-сервистері) талаптарға сәйкесуі: Қазақстан Республикасының электрондық құжат және электрондық цифрлық қолтаңба сұрақтары бойынша қолданыстағы заңнамасы, Тіркеу куәліктері саясаты және Ережелер;
- 3) Тіркеу куәліктері саясаты мен Ережелер талаптарын Интернет желісіндегі Банкінің ресми ақпараттық ресурсына жариялау.

175. Тіркеу орталығы қамтамасыз етеді:

- 1) Куәландырушы орталыққа жолданған тіркеу куәліктерін шығаруға сұраныстардағы деректердің сәйкестендіру процедурасы барысында өтініш беруші тапсырған құжаттардағы мәліметтерге сәйкестігі және бұл сұраныстарда әдейі немесе тіркеу орталығы қызметкерлерінің қателесіп жасаған әрекеттерінің нәтижесінде жіберілген қасақана немесе кездейсоқ бұрмаланулардың болмауы;
- 2) тіркеу орталығы қызметкерлері орындайтын процедуралардың келесі (тіркеу куәліктерін шығару және кері қайтарып алуға өтініштерді тіркеу және өңдеу, өтініш берушілерді сәйкестендіру процедуралары, тіркеу куәліктерін олардың иелеріне беру) талаптарға сәйкестігі: Қазақстан Республикасының электрондық құжат және электрондық цифрлық қолтаңба сұрақтары бойынша қолданыстағы заңнамасы, Тіркеу куәліктері саясаты және Ережелер.

176. Куәландырушы орталық және тіркеу орталықтары өз қызметінде Тіркеу куәліктері саясатының 9.6 параграфында мазмұндалған тіркеу куәліктері иелері мен пайдаланушыларының (жазылушы мен сенім білдіруші тараптың) кепілдіктері мен растауларының талаптарын орындайды.

9.7 параграф. КЕПІЛДІКТЕН БАС ТARTУ

177. Куәландырушы орталық тіркеу куәліктерінің иелері мен пайдаланушылары (жазылушылар және сенім білдіруші тараптар) алдында Қазақстан Республикасының электрондық құжат және электрондық цифрлық қолтаңба сұрақтары бойынша заңнамасында белгіленген және тіркеу куәліктерінің саясатында декларацияланған жауапкершіліктен басқа Банкілік қызметтер көрсету шарттарынан туындайтын қосымша жауапкершілік көтермейді, оның ішінде тауарлық жарамдылық пен сәйкестік үшін жауапкершілікпен қоса.

9.8 параграф. ЖАУАПКЕРШІЛІКТІ ШЕКТЕУ

178. Ашық кілттер инфрақұрылымына қатысушылар тікелей емес, ерекше, кездейсоқ немесе туындаған залал мен бос жіберілген пайда үшін жауап бермейді.

9.9 параграф. ӨТЕМДЕР

179. Қазақстан Республикасының қолданыстағы заңнамасына қарама-қайшы келмейтін бөлігінде, тіркеу орталықтары есебіне келесілер үшін өтемге байланысты шығыстар жатқызылады:

- 1) тіркеу куәліктерін шығаруға немесе кері қайтарып алуға өтініштердегі қате, адастырушы немесе қасақана жалған ақпаратты растағаны;
- 2) тіркеу куәліктерін шығаруға немесе кері қайтарып алуға өтініштерде көрсетілуге жататын елеулі фактілерді байқаусызда немесе қасақана жасырғаны.

9.10 параграф. КҮШНЕ ЕНУІ ЖӘНЕ ҚОЛДАНЫЛУЫНЫҢ ТОҚТАУЫ

180. Ережелер және оларға жасалған барлық өзгертулер мен толықтырулар Интернет желісіндегі Банкінің ресми ақпараттық ресурсында жарияланған күннен бастап күшіне енеді.

181. Оларға жарияланатын өзгерістер мен толықтыруларды ескере отырып Ережелер интернет желісіндегі Банкінің ресми ресурсында Ережелердің жаңа редакциясы жарияланған сәтке дейін күшін сақтайды.

182. Ережелердің күші жойылған жағдайда Куәландырушы орталық шығарған тіркеу куәліктерін пайдаланатын ақпараттық жүйелердің қатысушылары Тіркеу куәліктері саясатының талаптарымен тіркеу куәліктерінің қолданылу кезеңі аяқталғанға дейін байланысты болып қалады.

9.11 параграф. ЖЕКЕ ХАБАРЛАМА ЖӘНЕ ҚАТЫСУШЫЛАРМЕН БАЙЛАНЫС

183. Ашық кілттер инфрақұрылымына қатысушылар: Куәландырушы орталық, тіркеу орталықтары, тіркеу куәліктерінің иелері мен пайдаланушылары (жазылушылар және сенім білдіруші тараптар) - егер тараптар арасындағы келісімде өзгеше анықталмаған болса бір-бірімен байланыс үшін өзара іс-қимыл мәніне, коммуникацияның маңыздылығы мен жеделдігі дәрежесіне сәйкес келетін кез келген орынды арналарды пайдаланады.

9.12 параграф. ӨЗГЕРТУЛЕР МЕН ТОЛЫҚТЫРУЛАР

184. Ережелерге болымсыз өзгерістер (мекенжайлар мен сілтемелердің, байланыс ақпараттарының өзгеруі, қате жазуды түзету және т.б.) ашық кілттер инфрақұрылымына қатысушыларға алдын-ала хабарламастан енгізіледі. Өзгертулер мен толықтырулардың маңыздылық (маңызды немесе маңызсыз) деңгейі туралы шешімді Куәландырушы орталық өз бетінше қабылдайды.

185. Ережелерге жасалған маңызды өзгертулер мен толықтыруларды Куәландырушы орталық алдын ала жоба түрінде, әдетте күшіне енгенге дейін 14 күнтізбе күні бұрын интернет желісіндегі Банкінің ресми ресурсына жариялайды, егер Қазақстан Республикасының заңнамасында жарияланған өзгерістермен өзгеше көзделмесе.

9.13 параграф. ДАУЛАРДЫ ШЕШУ

186. Ашық кілттер инфрақұрылымына қатысушылар арасындағы: тіркеу куәліктерінің иелері мен пайдаланушылары (жазылушылар мен сенім білдіруші тараптар)

арасындағы, сондай-ақ бір жағынан жазылушы немесе сенім білдіруші тарап және екінші жағынан Куәландырушы орталық немесе тіркеу орталығы арасындағы даулар Қазақстан Республикасы заңнамасының қағидаларына сәйкес шешіледі.

187. Егер дау сотқа дейінгі тәртіпте шешілмесе, онда ол сот тәртібінде шешілуі тиіс.

9.14 параграф. ЮРИСДИКЦИЯ

188. Ережелердің мәні бойынша келіспеушіліктер нысанасы болып табылатын дауларды шешу үшін Қазақстан Республикасының заңнамасы қолданылады.

9.15 параграф. ҚОЛДАНЫСТАҒЫ ЗАҢНАМАҒА СӘЙКЕСТІК

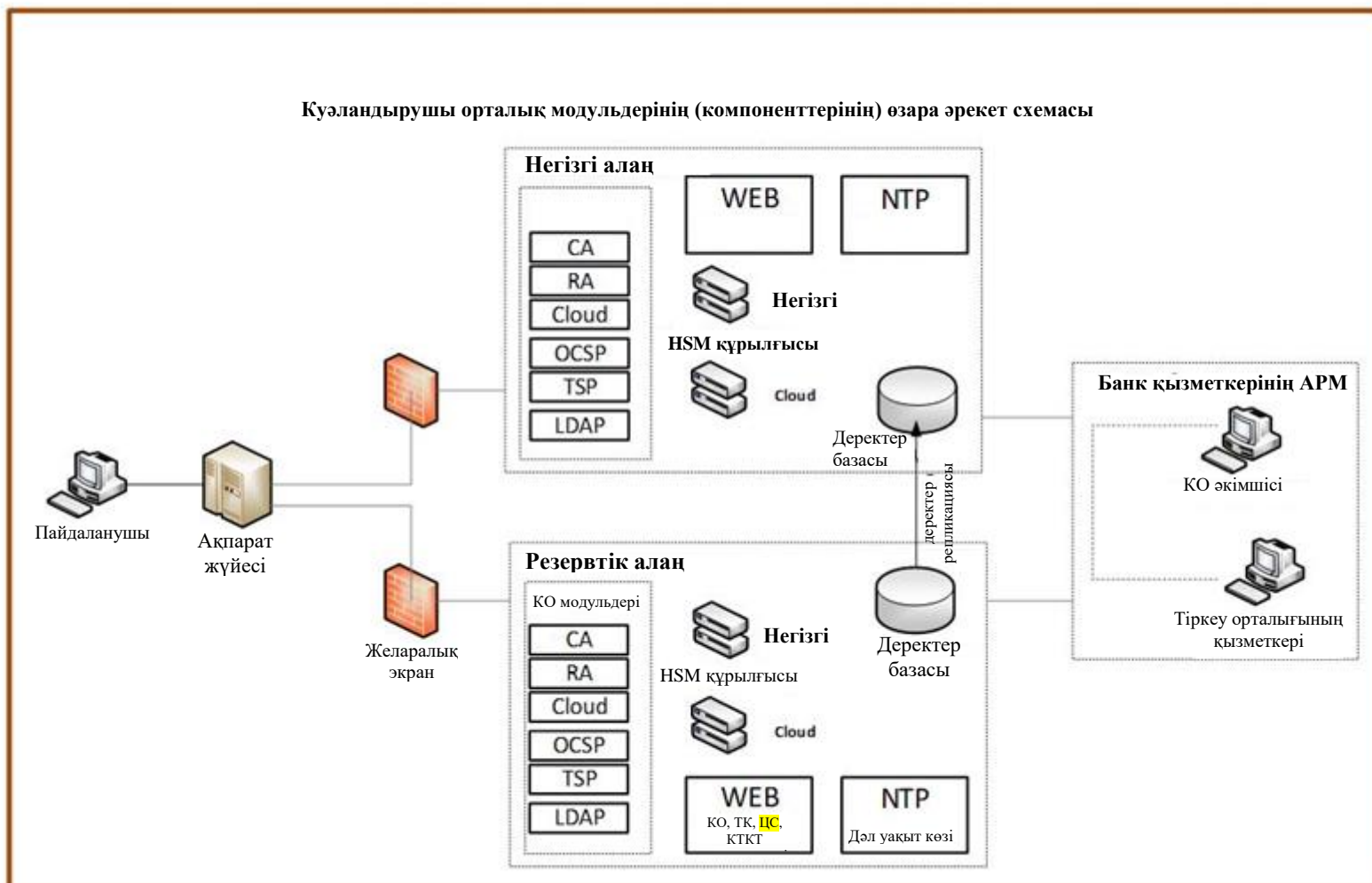
189. Ашық кілттер инфрақұрылымының қатысушыларына: Куәландырушы орталыққа, тіркеу орталықтарына, жазылушыларға және сенім білдіруші тараптарға – келесі сұрақтар бойынша Қазақстан Республикасы заңнамасының талаптары қолданылады:

- 1) электрондық құжат және электрондық цифрлық қолтаңба;
- 2) рұқсаттар мен хабарламалар (АКҚК жүзеге асыруға қатысты бөлімде);
- 3) төлемдер мен төлем жүйелері;
- 4) дербес деректер және оларды қорғау.

9.16 параграф. ӨЗГЕ ҚАҒИДАЛАР

190. Егер Ережелер қағидаларының бір бөлігін сот немесе уәкілетті мемлекеттік орган қолданылмайды деп таныған жағдайда, олардың қалған бөлігі күшін сақтайды.

191. Еңсерілмес күш (форс-мажор) мән-жайлары туындаған жағдайда ашық кілттер инфрақұрылымының қатысушылары: Куәландырушы орталық, тіркеу орталықтары, тіркеу куәліктерінің иелері мен пайдаланушылары (жазылушылар мен сенім білдіруші тараптар), – олардың арасында жасалған қолданыстағы шарттардың (егер бар болса) тиісті қағидаларын басшылыққа алады.



Куәландырушы орталық модульдерінің (компоненттерінің) өзара әрекет схемасына ТҮСІНІКТЕМЕ ЖАЗБА

Компоненттердің өзара әрекеті (негізгі және резервтік орталықр)

Куәландырушы орталықтың (әрі қарай – КО) ақпараттық жүйесі модульдерінің КО қоймасымен тіркеу куәліктерін, кері қайтарылып алынған тіркеу куәліктері тізімін жариялау және іздеу үшін өзара әрекеті LDAP хаттамасы бойынша жүзеге асырылады

КО-ның барлық модульдері NTP хаттамасы бойынша дәл уақыт көзінен алынатын бірдей уақытты пайдаланады.

КО модульдерінің өзара әрекетінің қауіпсіздігі РҚ СТ 1073-2007 сәйкес қауіпсіздіктің екінші деңгейіне сәйкесетін «ТУМАР-CSP» ақпаратты криптографиялық қорғаудың сертификатталған құралын пайдалану арқылы қамтамасыз етіледі.

КО жабық кілттерін сақтау және қауіпсіздігін қамтамасыз ету үшін РҚ СТ 1073-2007 сәйкес қауіпсіздіктің 2 деңгейіне сәйкесетін HSM қорғалған бағдарламалық-аппараттық кешендер пайдаланылады.

Тіркеу куәлігі иелерінің (жазылушылардың) жабық кілттерін жасау, сақтау және қауіпсіздігін қамтамасыз ету үшін ҚР СТ 1073-2007 сәйкес қауіпсіздіктің 3 деңгейіне сәйкес келетін HSM қорғалған бағдарламалық-аппараттық кешендері пайдаланылады.

Жүйеде барлық кіретін желілік трафикті бақылайтын және сүзетін желіаралық экрандар жұмыс істейді.

Деректерді өңдеу орталықтарының жұмысшы және резервтік серверлері арасындағы өзара әрекет

Деректерді сақтау және басқару MySQL ДББЖ арқылы қамтамасыз етіледі. Негізгі және резервтік орталықтар арасында нақты уақыт режимінде ДББЖ құралдарымен деректердің репликациясы орындалады, бұл жүйенің бұзылуға төзімділігін арттырады. Репликацияланатын деректерді қорғау TLS хаттамасын қолдана отырып, шифрлаумен қамтамасыз етіледі.

Пайдаланушылардың КО-мен өзара әрекеті

КО пайдаланушылары КО сервистерімен тікелей өзара әрекеттеспейді.

Өзара әрекет жасасу LDAP және HTTP (S) хаттамаларын пайдалана отырып, LDAP-қоймасымен және КО модульдерімен өзара әрекет жасау мүмкіндігі бар Банкінің мақсатты (қызмет көрсетілетін) ақпараттық жүйелері арқылы жүзеге асырылады.

КО қызметкерлерінің КО модульдерімен өзара әрекеті

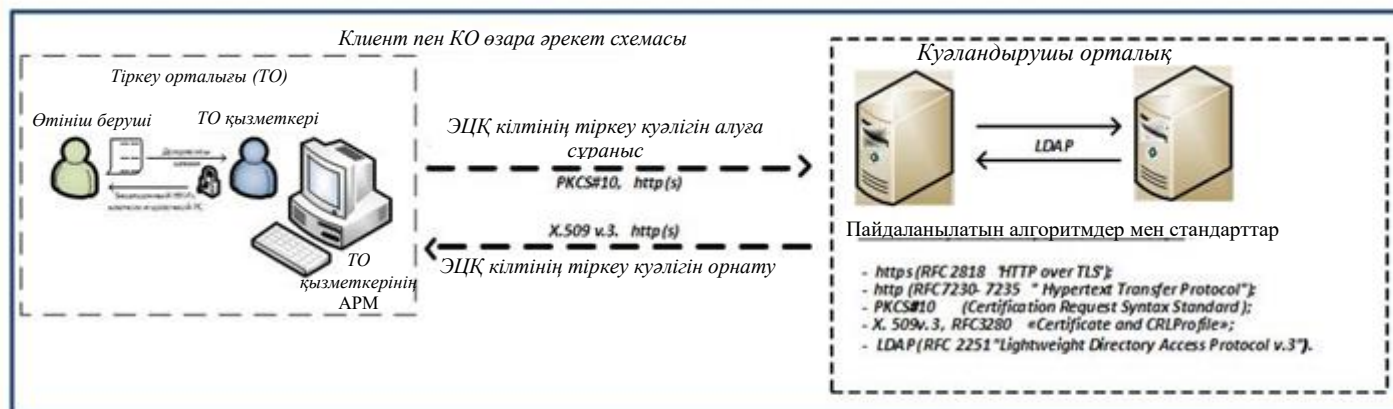
КО қызметкерлерінің КО модульдерімен өзара әрекеті LDAP және HTTP(S) хаттамаларын пайдаланы отырып, мамандандырылған бағдарламалық жасақтама арқылы жүзеге асырылады.

Қызметкердің жұмыс орнынан КО модульдеріне қол жеткізу белгілі бір қасиеттері бар қолданыстағы тіркеу куәлігі болған кезде ғана мүмкін болады.

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

Электрондық цифрлық қолтаңба қалыптастыру процесін жүзеге асыру бойынша және жекелеген параметрлер мен куәландырушы орталыққа қойылатын талаптармен криптографиялық түрлендірулердің қолданылатын алгоритмдері туралы деректермен және басқа бастапқы деректермен (негізгі талаптармен)

Электрондық цифрлық қолтаңба схемасы



Электрондық цифрлық қолтаңба қалыптастыру.... схемасы (жалғасы)

Куәландырушы орталық жағында тіркеу куәлігі иелерінің жабық кілттерін сақтау және пайдалану кезіндегі процестер ерекшеліктері

