



ІШКІ ҚҰЖАТ	
Атауы:	"Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін қолдану саясаты
Иесі:	Ақпараттық қауіпсіздік департаменті
Бекітілген:	Басқарманың шешімімен (06.09.2024 ж. № 103 хаттама)
Қолданысқа енгізу мерзімі:	6.09.2024
Соңғы өзгертулер/толықтырулар енгізу	Басқарманың 20.01.2026 №5 шешімімен бекітілген "Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін қолдану саясатына өзгерістер мен толықтырулар
Күші жойылған / күші жойылды деп танылған құжаттар (бар болса):	
Құпиялылық дәрежесі:	Жалпыға қол жетімді

МАЗМҰНЫ

1-ТАРАУ. ЖАЛПЫ ЕРЕЖЕЛЕР	4
1-БӨЛІМ. ҚҰЖАТТЫҢ АТАУЫ ЖӘНЕ СӘЙКЕСТЕНДІРІЛУІ.....	4
2-БӨЛІМ. ҰҒЫМДАР МЕН ҚЫСҚАРТУЛАР.....	4
3-БӨЛІМ. КО	6
4-БӨЛІМ. ТІРКЕУ КУӘЛІКТЕРІН ПАЙДАЛАНУ.....	6
5-БӨЛІМ. ҚҰЖАТТЫ БАСҚАРУ.....	7
6-БӨЛІМ. АҚПАРАТТЫ ЖАРИЯЛАУ	7
7-БӨЛІМ. АҚПАРАТТЫ ЖАРИЯЛАУ КЕЗЕҢІ.....	7
8-БӨЛІМ. ҚОҒАМДЫҚ АҚПАРАТҚА ҚОЛ ЖЕТКІЗУДІ БАҚЫЛАУ.....	7
2-ТАРАУ. ТІРКЕУ КУӘЛІКТЕРІНІҢ ШАБЛОНДАРЫ, КТКТ	7
1-БӨЛІМ. ТІРКЕУ КУӘЛІКТЕРІНІҢ СИПАТТАМАСЫ	7
2-БӨЛІМ. КТКТ СИПАТТАМАСЫ	11
3-БӨЛІМ. ОССР СИПАТТАМАСЫ.....	11
3-ТАРАУ. ҚОРЫТЫНДЫ ЕРЕЖЕЛЕР	11

**"Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін
қолдану саясаты, тірк. №A0-08-13/198/ПТ/06092024**

**"Фридом Банк Қазақстан" АҚ куәландырушы орталығының
тіркеу куәліктерін қолдану саясатына
бекітілген өзгерістер мен толықтырулар
ТІЗІЛІМІ**

№	Құжат нөмірі	Өзгерістер мен толықтыруларды бекіту туралы Банк органының шешімінің деректемелері	Бекітілген өзгерістер мен толықтыруларды қолданысқа енгізу мерзімі	Өзгерістер / толықтырулар енгізу негізі
1	№A0-08-13/198/ПТ/0609 2024	20.01.2026 жылғы №5 хаттама	21.01.2026ж	Уәкілетті органның ескертулерін жою үшін өзгерістер мен толықтырулар
2				
3				
4				
5				
6				

**"Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін
қолдану саясаты, тірк. №А0-08-13/198/ПТ/06092024**

1-ТАРАУ. ЖАЛПЫ ЕРЕЖЕЛЕР

1. Осы "Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін қолдану саясаты (бұдан әрі-Саясат) тіркеу куәліктерін басқару бөлігінде "Фридом Банк Қазақстан" АҚ куәландырушы орталығының жұмыс регламенті мен тетіктерін айқындайды.
2. Тіркеу куәліктерінің барлық иелері мен КО қызметкерлері үшін саясаттың талаптарын орындау міндетті.
3. Саясат Қазақстан Республикасының ЭЦҚ саласындағы заңнамасына және RFC 3647 ұсынымдарына, сондай-ақ КО ішкі және жария құжаттарына сәйкес әзірленді.
4. Саясат КО шығаратын тіркеу куәліктерінің түрлерін, оларды тексеру рәсімдерін, сондай-ақ оларды қолдану шарттарын айқындайды.
5. Тіркеу куәлігі ЭЦҚ ашық кілтінің мәнін ЭЦҚ тиісті жабық кілтін пайдаланатын пайдаланушыны сәйкестендіретін ақпаратпен байланыстырады.
6. Тіркеу куәлігін ЭЦҚ-ны тексеру үшін оны пайдаланушы немесе тіркеу куәліктерінен ЭЦҚ ашық кілтін қолдану қажет сенім білдірген Тарап қолданады.
7. Тіркеу куәлігіне сенім дәрежесі мынадай факторлармен айқындалады:
 - 1) КО қызметінің регламентімен;
 - 2) Қазақстан Республикасының ЭЦҚ саласындағы заңнамасымен.

1-БӨЛІМ. ҚҰЖАТТЫҢ АТАУЫ ЖӘНЕ СӘЙКЕСТЕНДІРІЛУІ

8. Құжаттың атауы: "Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін қолдану саясаты.

Нысан идентификаторы: 1.2.398.3.26.2 – "Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін қолдану саясаты.

Осы құжаттың өзекті редакциясы мына сілтеме бойынша қолжетімді:
<https://pki.bankffin.kz/policy/policy.pdf>.

2-БӨЛІМ. ҰҒЫМДАР МЕН ҚЫСҚАРТУЛАР

9. Осы Саясатта қолданылатын негізгі ұғымдар мен қысқартулар:
 - 1) Аппараттық криптографиялық модуль (Hardware Security Module) (бұдан әрі - HSM) - КО кілттерін, пайдаланушылардың ЭЦҚ жабық кілттерін генерациялауға, сақтауға, қорғауға және басқаруға арналған бағдарламалық-аппараттық модуль;
 - 2) Банк – "Фридом Банк Қазақстан" АҚ;
 - 3) Тіркеу куәлігінің иесі (пайдаланушысы) – атына тіркеу куәлігінде көрсетілген ашық кілтке сәйкес келетін жабық кілтті заңды түрде иеленетін тіркеу куәлігі берілген жеке тұлға немесе заңды тұлғаның уәкілетті өкілі;
 - 4) Ақпараттық қауіпсіздік департаменті (бұдан әрі – АҚД) – электрондық ақпараттық ресурстардың, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалу жай-күйін бақылауды қамтамасыз ететін Банктің құрылымдық бөлімшесі;
 - 5) Техникалық сипаттамалар мен стандарттарды, кеңінен қолданылатын Интернет желілерін қамтитын нөмірленген интернет-ақпараттық құжаттар сериясынан алынған құжат (Request for Comments) (бұдан әрі – RFC) 3647 – Internet X.509 ашық кілт инфрақұрылымына қойылатын талаптарды реттейтін IETF халықаралық стандарттар сериясынан ұсынылатын стандарт;
 - 6) Техникалық сипаттамалар мен стандарттарды, кеңінен қолданылатын Интернет желілерін қамтитын нөмірленген интернет-ақпараттық құжаттар сериясынан алынған құжат (Request for Comments) (бұдан әрі – RFC) 2560 – тіркеу куәлігінің мәртебесін анықтау үшін хаттамаға қойылатын талаптарды реттейтін IETF халықаралық стандарттар сериясынан ұсынылатын стандарт;
 - 7) Техникалық сипаттамалар мен стандарттарды, кеңінен қолданылатын Интернет желілерін қамтитын нөмірленген интернет-ақпараттық құжаттар сериясынан алынған құжат (Request for Comments) (бұдан әрі – RFC) 5280 – IETF (Internet Engineering Task Force,

**"Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін
қолдану саясаты, тірк. №А0-08-13/198/ПТ/06092024**

жобалаушылардың, ғалымдардың, желілік операторлардың және провайдерлердің ашық халықаралық қауымдастығы) халықаралық стандарттар сериясынан ұсынылатын стандарт, тіркеу куәліктері мен КТКТ құрылымына қойылатын талаптарды реттейді;

8) ЭЦҚ жабық кілті – электрондық цифрлық қолтаңба құралдарын пайдалана отырып, электрондық цифрлық қолтаңбаны жасауға арналған электрондық цифрлық таңбалар тізбегі;

9) Өтініш беруші – тіркеу куәлігін беруге немесе кері қайтарып алуға құжаттар берген жеке тұлға немесе заңды тұлға;

10) ЖСН – жеке сәйкестендіру нөмірі;

11) БСН – бизнес сәйкестендіру нөмірі;

12) КО Интернет-ресурсы – bankffin.kz;

13) Бұлтартпау – электрондық құжатты жөнелтушінің (автордың) тиісті құжатты немесе хабарламаны жіберу (қол қою) фактісінен бас тарту мүмкін еместігі. Бұлтартпаушылық электрондық құжаттың дұрыс екендігін, оны тіркеу куәлігінің иесі (авторлығы анықталған) жібергенін және растағанын, электрондық құжаттың мазмұнында жіберуші растағаннан кейін рұқсатсыз өзгерістер болмайтынын, электрондық құжатты растаған электрондық құжаттың авторы ол растаған электрондық құжаттың мазмұнымен келісетінін болжайды;

14) Негізгі ақпарат тасымалдаушысы – электрондық цифрлық қолтаңбаның сақталған жабық кілттерін қорғау үшін "Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар" ҚР СТ 1073-2007 стандартының талаптарына сәйкестік сертификаты бар АҚКҚ пайдаланылатын мамандандырылған тасымалдаушы;

15) Бұлтты ЭЦҚ – КО-ның HSM КО-да иесінің электрондық цифрлық қолтаңбасының жеке кілттерін жасауға, пайдалануға және сақтауға мүмкіндік беретін ақпараттық жүйесі, мұнда жеке кілтке қол жеткізуді иеленуші кемінде екі аутентификация факторы арқылы жүзеге асырады, олардың бірі биометриялық болып табылады;

16) Ашық кілт ЭЦҚ – кез келген тұлғаға қолжетімді және электрондық құжаттағы электрондық цифрлық қолтаңбаның түпнұсқалығын растауға арналған электрондық цифрлық таңбалар тізбегі;

17) КО қызметкері – КО БҚ, КО HSM, КО БҚ жұмыс істеуін қамтамасыз ететін платформаны әкімшілендіруге жауапты ақпараттық қауіпсіздік департаментінің қызметкері;

18) Тіркеу куәлігі – электрондық цифрлық қолтаңбаның Қазақстан Республикасының заңнамасында белгіленген талаптарға сәйкестігін растау үшін куәландырушы орталық беретін электрондық құжат;

19) Уақыт белгісі сервері – электрондық құжатқа уақыт белгісін қоюға арналған қызмет. Қызмет уақыт белгілерінің хаттамасы негізінде жұмыс істейді – Time-Stamp Protocol (TSP);

20) Кері қайтарып алынған тіркеу куәліктерінің тізімі (бұдан әрі –КТКТ) – қолданысы тоқтатылған тіркеу куәліктері туралы мәліметтерді, олардың сериялық нөмірлерін, қайтарып алу (күшін жою) күні мен себебін қамтитын тіркеу куәліктері тіркелімінің бөлігі;

21) Ақпаратты криптографиялық қорғау құралдары (бұдан әрі – АҚКҚ) – криптографиялық түрлендіру, кілттерді генерациялау, қалыптастыру, тарату немесе басқару алгоритмдерін іске асыратын және ақпараттық жүйелерде электрондық цифрлық қолтаңба мен шифрлауды қолдануды қамтамасыз ететін бағдарламалық-техникалық құралдардың жиынтығы. АҚКҚ дербес бағдарламалық модульдер түрінде де, қолданбалы бағдарламалық жасақтамаға енгізілген құралдар түрінде де қолданыла алады;

22) Куәландыру орталығы (бұдан әрі – КО) – электрондық цифрлық қолтаңбаның ашық кілтінің электрондық цифрлық қолтаңбаның жабық кілтіне сәйкестігін куәландыратын, тіркеу куәлігінің дұрыстығын растайтын "Фридом Банк Қазақстан" АҚ;

23) Электрондық цифрлық қолтаңба (бұдан әрі – ЭЦҚ) – электрондық цифрлық қолтаңба құралдарымен жасалған және электрондық құжаттың дұрыстығын, оның тиесілілігін және мазмұнының өзгермейтіндігін растайтын электрондық цифрлық таңбалар жиынтығы;

24) Электрондық құжат – ақпарат электрондық-цифрлық нысанда ұсынылған және электрондық цифрлық қолтаңба арқылы куәландырылған құжат;

**"Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін
қолдану саясаты, тірк. №А0-08-13/198/ПТ/06092024**

25) LDAP (Lightweight Directory Access Protocol) – International Telecommunication Union – Telecommunication sector (бұдан әрі – ITU-T) X. 500 ұсынымдарында әзірленген каталог қызметіне қол жеткізу үшін қолданбалы деңгей хаттамасы;

26) хэш – еркін ұзындықтағы кіріс массивін бекітілген ұзындықтың биттік жағына түрлендіру;

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

3-БӨЛІМ. КО

10. КО

КО келесі функцияларды орындайды:

- 1) тіркеу куәлігін беруге және кері қайтарып алуға сұрау салуларды алу және өңдеу;
- 2) тіркеу куәлігін беру, сақтау, кері қайтарып алу;
- 3) ЭЦҚ ашық кілтінің ЭЦҚ жабық кілтіне сәйкестігін куәландыру;
- 4) тіркеу куәліктерінің дұрыстығын растау;
- 5) КТКТ шығарылымы, жариялануы және қолдауы;
- 6) OSCP қызметіне сұраныстарды өңдеу және оны қолдау;
- 7) TSP уақыт белгісінің мөртабанын қою;
- 8) ЭЦҚ ашық кілттерін және ЭЦҚ жабық кілттерін жасау;
- 9) тіркеу куәліктерінің тізілімін жүргізу.

11. Қоғамдық ақпаратты сақтау және қол жетімділік

КО тәулігіне 24 сағат, аптасына 7 күн КО Интернет-ресурсында мынадай материалдардың жария қолжетімділігін қамтамасыз етеді:

- 1) MEMST алгоритмі бойынша КО түбірлік тіркеу куәлігі;
- 2) MEMST алгоритмі бойынша ҚР түбірлік куәландырушы орталығының түбірлік тіркеу куәлігі;
- 3) КО қызметінің регламенті;
- 4) КО тіркеу куәліктерін қолдану саясаты;
- 5) КТКТ;
- 6) OSCP қызметтері;
- 7) TSP қызметі.

12. Сенімді тарап

Сенімді тарап – тіркеу куәліктері қолданылатын ақпараттық жүйелер:

- 1) Банктің жеке және / немесе заңды тұлғалары үшін Интернет-банкінг (оның ішінде клиенттер банк қызметтерін пайдаланатын мобильді қосымшалар);
- 2) Certex Cloud жүйесі (бұлтты ЭЦҚ).

4-БӨЛІМ. ТІРКЕУ КУӘЛІКТЕРІН ПАЙДАЛАНУ

13. Тіркеу куәлігін рұқсат етілген пайдалану

Тіркеу куәлігі КО бекіткен АЖ-да, ЭЦҚ электрондық құжаттарына қол қою үшін, КО бекіткен ақпараттық жүйелерде банк клиенттерін сәйкестендіру және/немесе аутентификациялау үшін, сондай-ақ ЭЦҚ түпнұсқалығын тексеру үшін пайдаланылады.

14. Тіркеу куәліктерін пайдалануды шектеу

Тіркеу куәліктері саясаттың осы бөлімінің 13-тармағында сипатталмаған өзге де жағдайларда, сондай-ақ олар қайтарып алынған немесе жарамсыз болған жағдайда олардың қолданылу мерзімі аяқталғаннан кейін пайдаланыла алмайды.

Тесттік тіркеу куәліктері заңды маңызы жоқ электрондық құжаттардың ЭЦҚ-на қол

**"Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін
қолдану саясаты, тірк. №А0-08-13/198/ПТ/06092024**

қою үшін ғана пайдаланылуға тиіс.

5-БӨЛІМ. ҚҰЖАТТЫ БАСҚАРУ

15. Құжаттың мазмұнына жауапты ұйым

"Фридом Банк Қазақстан" АҚ.

16. Байланыс ақпараты

"Фридом Банк Қазақстан" АҚ, Қазақстан Республикасы, 050000, Алматы қ., Алмалы ауданы, Құрманғазы к-сі, 61 үй, телефон: 595, +7 776 159 55 95.

17. Өзгерістерді бекітетін орган

Құжаттағы өзгерістерді "Фридом Банк Қазақстан" АҚ Басқармасы бекітеді.

18. Өзгерістерді бекіту рәсімі

Саясатты жаңа редакцияда бекіту туралы немесе оған өзгерістер мен толықтырулар енгізу туралы тіркеу куәліктері иелерінің ресми хабарламасы саясатты жаңа редакцияда КО Интернет-ресурсында мына мекенжай бойынша жариялау болып табылады: <https://pki.bankffin.kz/policy/policy.pdf>.

Саясатқа енгізілетін барлық өзгерістер күшіне енеді және тіркеу куәліктерінің иелері олар жарияланғаннан кейін дереу орындауға міндетті болады.

КО саясатын жариялау ол бекітілгеннен кейін 3 (үш) жұмыс күні ішінде жүзеге асырылады.

6-БӨЛІМ. АҚПАРАТТЫ ЖАРИЯЛАУ

19. КО КТКТ RFC 5280 ұсынымдарымен және осы Саясатпен айқындалған электрондық нысанда және форматта ұсынылады. КО MEMCT алгоритмінде тіркеу куәліктері үшін КТКТ жариялайды.

20. КО сонымен қатар АЖ қатысушыларына OSCP қызметі арқылы тіркеу куәліктерінің мәртебесін анонимді тексеру қызметін ұсынады.

21. КО TSP қызметі арқылы АЖ қатысушыларына "Уақыт мөртабанын" жеткізуді анонимді тексеру қызметін ұсынады.

21-1. Оқиға хаттамалары күн сайын хэшке айналады және хэш деректері блокчейн оқиғалар тізбегінде сақталады. Бұл үшін қолданылатын блокчейн Интернетте қол жетімді. <https://my.bankffin.kz/digital-signature/blockchain/?limit=100&offset=0>.

7-БӨЛІМ. АҚПАРАТТЫ ЖАРИЯЛАУ КЕЗЕҢІ

22. КТКТ жариялау кезеңі тәулігіне 1 рет.

8-БӨЛІМ. ҚОҒАМДЫҚ АҚПАРАТҚА ҚОЛ ЖЕТКІЗУДІ БАҚЫЛАУ

23. КО-да санкцияланбаған өзгерістер енгізуді болдырмау немесе КТКТ және КО-да қамтылған ақпаратты жою мақсатында ақпараттық және физикалық қауіпсіздік шаралары іске асырылды.

2-ТАРАУ. ТІРКЕУ КУӘЛІКТЕРІНІҢ ШАБЛОНДАРЫ, КТКТ

1-БӨЛІМ. ТІРКЕУ КУӘЛІКТЕРІНІҢ СИПАТТАМАСЫ

24. Тіркеу куәлігінің нұсқасы

RO ITU-T X. 509v3 және RFC 5280 ұсынымдарына негізделген форматта электрондық нысанда тіркеу куәлігін береді (Certificate and Certificate Revocation List (CRL) Profile).

"Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін қолдану саясаты, тірк. №А0-08-13/198/ПТ/06092024

25. Тіркеу куәліктерін кеңейту

Тіркеу куәліктері мынадай толықтыруларды қамтуы мүмкін:

authorityKeyIdentifier	КО уәкілетті тұлғасының кілт идентификаторы
subjectKeyIdentifier	Тіркеу куәлігі иесінің кілт идентификаторы
ExtendedKeyUsage	Электрондық цифрлық қолтаңбасы бар электрондық құжат заңды мәнге ие болатын кілтті пайдалану саласы (салалары). Мүмкін мәндер: Client Authentication, Secure e-mail, Time stamping, IPSec (Tunnel, User)
KeyUsage	Кілттің мақсаты. Мүмкін мәндер: Тіркеу куәлігіне қол қою, Офлайн шолу тізіміне қол қою (CRL), Кері байланыс тізіміне қол қою (CRL), Сандық қолтаңба, Бұлтартпау, Кілттерді шифрлау, Деректерді шифрлау
Basic constraints	Субъект түрі
cRLDistributionPoint	Күшін жойған (кері қайтарып алынған) тіркеу куәліктерінің тізімін тарату нүктесі
certificatePolicies	Тіркеу куәліктерінің саясаты
Authority Information Access (optional)	Тіркеу куәлігінің мәртебесі туралы ақпарат алу тәсілі

26. Алгоритмнің объектілік идентификаторлары

КО ЭЦҚ құралы алгоритмдерінің мынадай идентификаторларын пайдаланады:

MEMCT 34.310-2004	iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) sign(2)
MEMCT 34.311-95	iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) hash(1)

27. Құрылымы түбірлік КО тіркеу куәлігі (алгоритм MEMCT 34.310-2004)

Атауы	Мазмұны
Нұсқа	V3
Сериялық нөмір	Тіркеу куәлігінің бірегей сериялық нөмірі
Қол қою алгоритмі	MEMCT 34.310 қол қою алгоритмі
Жеткізуші	CN = Freedom Root Certificate Authority; O = Freedom Bank Kazakhstan JSC; C = KZ
Субъект	CN = Freedom Root Certificate Authority; O = Freedom Bank Kazakhstan JSC; C = KZ
Жарамдылық мерзімі	бастап жарамды: DDMMYYYYHHMMSSZ GMT дейін жарамды: DDMMYYYYHHMMSSZ GMT

"Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін қолдану саясаты, тірк. №А0-08-13/198/ПТ/06092024

Ашық кілт алгоритмі	Алгоритмнің объект идентификаторы
Ашық кілт	Екілік түрдегі ашық кілт мәні
Тіркеу куәлігін кеңейту	Тіркеу куәлігін толықтыру
Қолы	ЭЦҚ

28. Жеке тұлғалар үшін бұлтты ЭЦҚ (MEMCT 34.310-2004 алгоритмі) пайдаланатын тіркеу куәлігі иесінің тіркеу куәлігінің құрылымы

Атауы	Мазмұны
Нұсқа	V3
Сериялық нөмір	Тіркеу куәлігінің бірегей сериялық нөмірі
Қол қою алгоритмі	MEMCT 34.310 қол қою алгоритмі
Жеткізуші	CN = Freedom Root Certificate Authority; O = Freedom Bank Kazakhstan JSC; C = KZ
Субъект	CN = Т.А.Ә. (Тегі Аты Әкесінің аты) SERIALNUMBER = ЖСН (Жеке сәйкестендіру нөмірі); OU = БСН (Бизнес-сәйкестендіру нөмірі) – заңды тұлға үшін; O = Freedom Bank Kazakhstan JSC; C = KZ
Жарамдылық мерзімі	DDMMYYYYHHMMSSZ GMT бастап жарамды DDMMYYYYHHMMSSZ GMT дейін жарамды
Ашық кілт алгоритмі	Алгоритмнің объект идентификаторы
Ашық кілт	Екілік түрдегі ашық кілт мәні
Тіркеу куәлігін кеңейту	Тіркеу куәлігін толықтыру
Қолы	ЭЦҚ

28-1. Заңды тұлғалар үшін бұлтты ЭЦҚ пайдаланатын тіркеу куәлігі иесінің тіркеу куәлігінің құрылымы (MEMCT 34.310-2004 алгоритмі)

Атауы	Мазмұны
Нұсқа	V3
Сериялық нөмір	Тіркеу куәлігінің бірегей сериялық нөмірі
Қол қою алгоритмі	MEMCT 34.310 қол қою алгоритмі
Жеткізуші	CN = Freedom Root Certificate Authority; O = Freedom Bank Kazakhstan JSC; C = KZ
Субъект	CN = Т.А.Ә. (Тегі Аты Әкесінің аты) SERIALNUMBER = IIN (Жеке Сәйкестендіру Нөмірі); OU = BIN (Бизнес сәйкестендіру нөмірі) – заңды тұлға үшін; O = Freedom Bank Kazakhstan JSC; C = KZ
Жарамдылық мерзімі	DDMMYYYYHHMMSSZ GMT бастап жарамды DDMMYYYYHHMMSSZ GMT дейін жарамды

"Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін қолдану саясаты, тірк. №А0-08-13/198/ПТ/06092024

Ашық кілт алгоритмі	Алгоритмнің объект идентификаторы
Ашық кілт	Екілік түрдегі ашық кілт мәні
Тіркеу куәлігін кеңейту	Тіркеу куәлігін толықтыру
Қолы	ЭЦҚ

29. Атауларға қойылатын шектеулер (сәйкестендіру деректері)

Сәйкестендіру деректеріне ITU-T X.501 (Distinguished Names) сәйкес мазмұн, жол ұзындығы және пайдаланылған таңбалар бойынша шектеулер қойылады.

КО қызметкерінің сәйкестендіру деректері өрісінің міндетті атрибуттары:

Common Name	Т.А.Ә. (Тегі Аты Әкесінің аты)
SERIALNUMBER	ЖСН (Жеке сәйкестендіру нөмірі)
OU	БСН (Бизнес-сәйкестендіру нөмірі)
Organization Unit	Банктің құрылымдық бөлімшесінің атауы
Organization	Freedom Bank Kazakhstan (жұмыс орнының атауы)
Country	KZ

Банк клиентінің сәйкестендіру деректері өрісінің міндетті атрибуттары:

Common Name	Т.А.Ә. (Тегі Аты Әкесінің аты)
SERIALNUMBER	ЖСН (Жеке сәйкестендіру нөмірі)
OU	БСН (Бизнес-сәйкестендіру нөмірі)
Organization	Freedom Bank Kazakhstan JSC
Country	KZ

Бұлтты ЭЦҚ пайдаланушысы болып табылатын тіркеу куәлігі иесінің сәйкестендіру деректері өрісінің міндетті атрибуттары:

Common Name	Т.А.Ә. (Тегі Аты Әкесінің аты)
SERIALNUMBER	ЖСН (Жеке сәйкестендіру нөмірі)
OU	БСН (Бизнес-сәйкестендіру нөмірі)
Organization	Freedom Bank Kazakhstan JSC;
Country	KZ

30. Тіркеу куәліктері саясатының объектілік идентификаторы

КО RFC 5280 сәйкес тіркеу куәліктерін береді (3 нұсқа X.509 тіркеу куәлігі). Берілген тіркеу куәліктері осы тіркеу куәлігі үшін тіркеу куәліктерінің бір немесе одан да көп саясаты қолданылғанын мәлімдейтін жолдарды қамтиды. Тіркеу куәлігінің шығарушысы да, иесі де тануы тиіс тіркеу куәлігінің саясаты бірегей және тіркелген Object Identifier тіркеу куәлігінде берілген. Тіркеу куәлігінің саясатын мүдделі тұлға тіркеу куәлігіне және онда қамтылған ақпаратқа нақты ақпараттық жүйе үшін сене ала ма деген мәселені шешкен кезде қолдана алады. Сенім білдіруші Тарап өзінің БҚ алдын-ала конфигурациялайды, сондықтан ол қандай саясатты қажет ететінін "біледі" және сәйкесінше, егер талап етілетін саясат болмаса, тіркеу куәліктеріне сенбейді.

Тесттік тіркеу куәліктері үшін осы құжатта көрсетілген стандартты саясат енгізіледі. Тестілеуге арналған тестілік тіркеу куәліктері КО-ның тестілік жабдықтарында (HSM) шығарылады, электрондық құжаттардың заңдық маңыздылығын қамтамасыз етпейді және сенім білдіруші тарап тестілік ақпараттық/Қаржы жүйелерінде тестілік тіркеу куәліктері ретінде ғана пайдалана алады. Тесттік тіркеу куәліктерін алу үшін өтініш берушіге аутентификация рәсімінен өтудің қажеті жоқ.

**"Фридом Банк Қазақстан" АҚ куәландырушы орталығының тіркеу куәліктерін
қолдану саясаты, тірк. №A0-08-13/198/ПТ/06092024**

2-БӨЛІМ. КТКТ СИПАТТАМАСЫ

31. Нұсқа нөмірі

КТКТ электронды түрде және белгілі бір RFC 5280 форматында беріледі. КТКТ КО түбірлік тіркеу куәлігімен куәландырылады. КТКТ қол жетімділігі LDAP және HTTP протоколдары арқылы қамтамасыз етіледі.

32. Кері қайтарып алынған тіркеу куәліктері тізімінің құрылымы (КТКТ) (MEMСТ 34.310-2004 алгоритмі)

Атауы	Мазмұны
Нұсқа	V2
Жеткізуші	CN = Freedom Root Certificate Authority; O = Freedom Bank Kazakhstan JSC; C = KZ
Шығарылған күні	бастап жарамды: DDMMYYYYHHMMSSZ GMT
Жаңарту күні	дейін жарамды: DDMMYYYYHHMMSSZ GMT
КТКТ кеңейтімдері	КТКТ толықтырулары
Кері қайтарып алынған тіркеу куәліктері	Келесі түрдің реттілігі: • CertificateSerialNumber (тіркеу куәлігінің сериялық нөмірі) • Time (тіркеу куәлігін қайтарып алуға өтінішті өңдеу күні мен уақыты)
Қол қою алгоритмі	MEMСТ 34.310 қол қою алгоритмі
Қолы	ЭЦҚ

3-БӨЛІМ. OSCP СИПАТТАМАСЫ

33. OSCP хаттамасы сенім білдірілген тараптарға ағымдағы уақытта тіркеу куәлігінің мәртебесін анықтау үшін қажет – қайтарып алынды ма, жоқ па. OSCP КТКТ көмегімен мүмкін болғаннан гөрі тіркеу куәліктерін қайтарып алу туралы уақтылы ақпарат алуға қатысты талаптарды қамтамасыз ету үшін пайдаланылуы мүмкін.

34. Нұсқа нөмірі

Тіркеу куәлігінің мәртебесін тексеру үшін KO RFC 2560 Online Certificate Status Protocol – OSCP ұсынымдарына сәйкес OSCP 1 нұсқасын пайдаланады.

35. OSCP кеңейтімдері

OSCP қызметі өндейтін кеңейтімдер, сондай – ақ олардың сыни деңгейі RFC 2560 Online Certificate Status Protocol-OSCP ұсыныстарына сәйкес келеді.

3-ТАРАУ. ҚОРЫТЫНДЫ ЕРЕЖЕЛЕР

36. Саясатқа өзгерістер мен толықтырулар енгізу КО ішкі нормативтік құжаттарының талаптарына сәйкес жүзеге асырылады.

37. Саясат Интернет-ресурста жарияланған сәттен бастап күшіне енеді және саясаттың жаңа редакциясы жарияланғанға дейін қолданылады.

38. Саясатқа өзгерістер енгізуге АҚД жауапты.

39. АҚД директоры осы Саясат талаптарының сақталуын бақылауға жауапты.

40. Осы саясатты қайта қарау жоспарлы да, жоспардан тыс та болуы мүмкін – қолданыстағы заңнамадағы немесе банк бөлімшелерінің жұмыс технологиясындағы өзгерістерге, аудиторлардың ұсыныстары мен ескертулеріне, сыртқы сарапшылардың ұсыныстарына байланысты. Онда баяндалған ақпаратты талдау және өзектендіру мақсатында осы саясатты міндетті түрде қайта қарау кемінде екі жылда бір рет жүзеге асырылуға тиіс.

41. Осы Саясат Банктің барлық қызметкерлері мен тіркеу куәліктерінің иелеріне орындау және танысу үшін міндетті.