Куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін сақтау қағидаларын бекіту туралы

Қазақстан Республикасы Премьер-Министрінің орынбасары – Жасанды интеллект және цифрлық даму министрінің 2026 жылғы 11 тамыздағы № 474/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2026 жылғы 12 тамызда № 39573 болып тіркелді

Қазақстан Республикасы Цифрлық кодексінің 51-бабының 3-тармағының төртінші бөлігіне сәйкес БҰЙЫРАМЫН:

1. Қоса беріліп отырған куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін сақтау қағидалары бекітілсін.

2. Мыналардың:

1) "Куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін жасау, пайдалану және сақтау қағидаларын бекіту туралы" Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2020 жылғы 27 қазандағы № 405/НҚ бұйрығының (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 21549 болып тіркелген);

2) "Куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін жасау, пайдалану және сақтау қағидаларын бекіту туралы" Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2020 жылғы 27 қазандағы № 405/НҚ бұйрығына өзгерістер енгізу туралы" Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2023 жылғы 17 наурыздағы № 95/НҚ бұйрығының (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 32129 болып тіркелген) күші жойылды деп танылсын.

3. Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің Цифрлық шешімдер департаменті Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрық ресми жарияланғаннан кейін оны Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің интернет-ресурсында орналастыруды;

3) осы бұйрық Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің Заң департаментіне осы тармақтың 1) және 2) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтерді ұсынуды қамтамасыз етсін.

4. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Жасанды интеллект және цифрлық даму вице-министріне жүктелсін.

5. Осы бұйрық алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

Қазақстан Республикасы
Премьер-Министрінің орынбасары –
Жасанды интеллект және цифрлық даму министрі *Ж. Мадиев*

"КЕЛІСІЛДІ"
Қазақстан Республикасының
Сауда және интеграция министрлігі
"КЕЛІСІЛДІ"
Қазақстан Республикасының
Ұлттық қауіпсіздік комитеті

Қазақстан Республикасы
Премьер-Министрінің
орынбасары – Жасанды
интеллект және цифрлық
даму министрі
2026 жылғы 11 тамыздағы
№ 474/НҚ Бұйрығымен
бекітілген

Куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін сақтау қағидалары

1-тарау. Жалпы ережелер

1. Осы Куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін сақтау қағидалары (бұдан әрі – Қағидалар) Қазақстан Республикасы Цифрлық Кодексінің (бұдан әрі – Кодекс) 51-бабы 3-тармағының төртінші бөлігіне сәйкес әзірленді және куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін сақтау тәртібін айқындайды

2. Осы Қағидаларда мынадай ұғымдар қолданылады:

1) аппараттық криптографиялық модуль (Hardware Security Module) (бұдан әрі – HSM) – криптографиялық кілттерді жасау, пайдалану және сақтау, сондай-ақ оларды пайдалана отырып криптографиялық операцияларды орындау кезінде олардың қауіпсіздігін қамтамасыз етуге арналған аппараттық модуль;

2) биометриялық аутентификация – жеке тұлғаны анықтау мақсатында биометриялық деректердің сәйкестігін салыстыру мен тексеру процесі;

3) бұлтты электрондық цифрлық қолтаңбаның жабық кілті (бұдан әрі – бұлтты ЭЦҚ жабық кілті) – электрондық цифрлық қолтаңбаның жабық кілттерінің бұлтты сақтау

орнында құрылатын, сақталатын және пайдаланылатын электрондық цифрлық қолтаңбаның жабық кілті;

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

5) куәландырушы орталық (бұдан әрі – КО) – Қазақстан Республикасының заңнамасына сәйкес құрылған, электрондық цифрлық қолтаңбаның ашық кілттері сертификаттарының анықтығын, электрондық цифрлық қолтаңбаның ашық кілттерінің тиесілілігі мен жарамдылығын растайтын заңды тұлға;

6) қорғалған негізгі ақпаратты тасымалдаушы – онда сақталатын электрондық цифрлық қолтаңбаның жабық кілттерін қорғау үшін Қазақстан Республикасының ҚР СТ 1073-2007 "Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар" немесе ҚР СТ 1073-2025 "Ақпараттық қауіпсіздікке және өмірлік цикл процестеріне қойылатын талаптар" ұлттық стандарттарының талаптарына сәйкестік сертификаты бар ақпаратты криптографиялық қорғау құралдары пайдаланылатын арнайы жеткізгіш;

7) хэш – деректерден алынатын және олардың тұтастығын тексеру үшін қолданылатын тіркелген ұзындықтың мәні;

8) электрондық цифрлық қолтаңба (бұдан әрі – ЭЦҚ) – электрондық цифрлық қолтаңбаның жабық кілті мен электрондық цифрлық қолтаңба құралдарын пайдалана отырып жасалған, электрондық құжаттың анықтығын, оның тиесілілігін және мазмұнының өзгермейтіндігін растайтын цифрлық жазба (цифрлық деректер жиынтығы);

9) электрондық цифрлық қолтаңба құралдары – электрондық цифрлық қолтаңбаны жасау және оның түпнұсқалығын тексеру үшін пайдаланылатын бағдарламалық қамтамасыз ету мен цифрлық инфрақұрылым объектілерінің жиынтығы;

10) электрондық цифрлық қолтаңбаның ашық кілті – электрондық цифрлық қолтаңбаның түпнұсқалығын растауға арналған цифрлық деректер;

11) электрондық цифрлық қолтаңбаның ашық кілті сертификатының иесі (бұдан әрі – иесі) – атына электрондық цифрлық қолтаңбаның ашық кілті сертификатында көрсетілген ашық кілтке сәйкес келетін жабық кілтті заңды түрде меңгерген, электрондық цифрлық қолтаңбаның ашық кілті сертификаты берілген жеке немесе заңды тұлға;

12) электрондық цифрлық қолтаңбаның ашық кілті сертификаты (бұдан әрі – сертификаты) – куәландырушы орталықтың электрондық цифрлық қолтаңбасымен

куәландырылған цифрлық жазба, ол электрондық цифрлық қолтаңбаның Қазақстан Республикасының Цифрлық Кодексінде белгіленген талаптарға сәйкестігін растауға қызмет етеді;

13) электрондық цифрлық қолтаңбаның жабық кілттерінің бұлтты сақтау орны (бұдан әрі – бұлтты сақтау орны) – көп факторлы аутентификациядан өткеннен кейін факторларының бірі биометриялық қолтаңба болып табылатын, куәландырушы орталықтың аппараттық криптографиялық модулінде иесіне электрондық цифрлық қолтаңбаның жабық кілттерін жасауға, сақтауға, пайдалануға және жоюға мүмкіндік беретін куәландырушы орталықтың сервисі;

14) электрондық цифрлық қолтаңбаның жабық кілті – электрондық цифрлық қолтаңба құралдарын пайдалана отырып, электрондық цифрлық қолтаңбаны жасауға арналған цифрлық деректер.

2-тарау. Куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін сақтау тәртібі

3. Бұлтты ЭЦҚ жабық кілті КО бұлтты сақтау орнында жасалады.

4. Бұлтты ЭЦҚ жабық кілті HSM ішінде қатаң түрде генерацияланады және бұлтты бұлтты ЭЦҚ жабық кілті HSM-ден ашық түрде алынбайды.

Бұл ретте HSM:

1) Қазақстан Республикасының ҚР СТ 1073-2007 "Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар" немесе ҚР СТ 1073-2025 "Ақпараттық қауіпсіздікке және өмірлік цикл процестеріне қойылатын талаптар" ұлттық стандартының талаптарына сәйкес қауіпсіздік деңгейі үшінші деңгейден төмен емес;

2) HSM корпусының тұтастығы бұзылған кезде КО электрондық цифрлық қолтаңбаның жабық кілттерін автоматты түрде алып тастаумен ашу датчиктерін пайдалануды көздейтін периметрді физикалық қорғаумен (корпусты ашудан қорғау) жобаланған.

5. ЭЦҚ бұлтты жабық кілттерін архивтеу негізгі жабдық істен шыққан кезде, апаттық жағдайларда, HSM жұмыс қабілеттілігінен айырылған кезде, сондай-ақ жабдықты ауыстыру, жаңғырту немесе көшіру жөніндегі іс-шараларды жүргізу кезінде бұлтты сақтаудың жұмыс қабілеттілігін қалпына келтіруді қамтамасыз ету мақсатында жүзеге асырылады.

HSM ЭЦҚ бұлтты жабық кілттерін архивтеуде тек шифрланған түрде, N-нан M схемасы бойынша (5-тен кемінде 3) шифрлау кілтін бөлу тетігін қолдана отырып жүзеге асыруға жол беріледі, оның бөліктері ақпараттың кілттік қорғалған жеткізгіштерінде сақталады. Резервтік жабдықта архивтен қалпына келтіру N құрамдас бөліктерінің кемінде M болған жағдайда ғана жол беріледі.

N компоненттерінің M соңғы тәуелділігі кез-келген қалпына келтіру сценарийі үшін сақталған жағдайда, кілттерді басқарудың көп деңгейлі схемасына рұқсат етіледі.

ЭЦҚ бұлтты жабық кілттерінің архивтік көшірмелері осы Қағидалардың 8-тармағында көзделген жағдайларда ЭЦҚ тиісті бұлтты жабық кілттері жойылғанға дейін сақталады.

ЭЦҚ бұлтты жабық кілттерінің архивтік көшірмелерін жою куәландырушы орталықтың ішкі құжаттарында белгіленген тәртіппен жүзеге асырылады.

6. ЭЦҚ бұлтты жабық кілтін жасау және сертификат шығару кезінде өтініш беруші:

1) дербес деректерді жинауға және өңдеуге келісім береді;

2) ЭЦҚ бұлтты жабық кілтін жасау кезінде адамның бейнесі тікелей жүзеге асырылатын фотосуретті, бейнежазбаны немесе өзге де имитациялық материалды пайдалануды болдырмау үшін оның тірі адамға тиесілі екенін растай отырып, адамның бейнесі негізінде биометриялық аутентификацияны қамтитын көп факторлы аутентификациядан өтеді;

3) ЭЦҚ бұлтты жабық кілтіне пароль орнатады.

Құпия сөзді қорғалған сақтауды және оған қол жеткізуді бақылауды қамтамасыз ететін пайдаланушы құрылғысының кіріктірілген құралдарын пайдалануға рұқсат етіледі.

7. Жасалған бұлтты ЭЦҚ жабық кілті HSM шифрланған түрде сақталады. ЭЦҚ бұлтты жабық кілтін криптографиялық қорғау үшін пайдаланылатын құпия мән ретінде куәландырушы орталықта сақталмайтын иесі белгілеген пароль қолданылады. Парольді тексеру үшін HSM оның хэшін сақтайды. Пароль қалпына келтірілмейді. Пароль жоғалған жағдайда бұлтты ЭЦҚ тиісті жабық кілтін пайдалануға жол берілмейді.

8. Бұлтты ЭЦҚ жабық кілті бұлтты сақтау орнынан мынадай жағдайда:

1) бұлтты ЭЦҚ жабық кілті сертификатын қайтарып алу кезінде;

2) бұлтты ЭЦҚ жабық кілті сертификатының қолданылу мерзімі өткен кезде жойылады.

9. Бұлтты ЭЦҚ жабық кілтін пайдалану иесінің парольді растауды және фотосуретті , бейнежазбаны не өзге де имитациялық материалды пайдалануды болдырмайтын, тұлға бейнесінің тірі адамға тиесілі екенін растау арқылы бет бейнесі негізінде жүзеге асырылатын биометриялық аутентификацияны қамтитын көп факторлы аутентификациядан өткеннен кейін жүзеге асырылады.

10. Электрондық құжаттарға қол қою HSM жадында қол қойылған файлды немесе оның хэшін HSM жіберу арқылы жүзеге асырылады. Берілетін деректерге қол қою операциясы аяқталғаннан кейін сақтауға жатпайды.

11. КО иесінің аутентификациясы кезінде аутентификация деректерін беру шифрланған түрде жүзеге асырылады, бұл ретте оларды шифрлау иесінің тарапында дербес компьютерді не мобильді құрылғыны пайдалану арқылы жүзеге асырылады.

12. Сертификат иесінің ЭЦҚ бұлтты жабық кілтінің компрометациялау фактісі анықталған жағдайда КО ЭЦҚ сертификатын кері қайтарып алады және кері қайтарып алынған ЭЦҚ сертификаттарының келесі тізімінде және ЭЦҚ сертификатының кері

қайтарып алу мәртебесін тексеру онлайн-сервисінде кері қайтарып алу туралы ақпаратты жариялайды.

13. КО келесі оқиғаларды хаттамалауды қамтамасыз етеді:

1) бұлтты ЭЦҚ жабық кілтін қалыптастыру;

2) бұлтты ЭЦҚ жабық кілтін пайдалану;

3) бұлтты ЭЦҚ жабық кілтін жою (өшіру).

Оқиғалар хаттамаларын сақтау мерзімі сертификаттың қолданылу мерзімі өткен күннен бастап 3 (үш) жылды құрайды.

Іс-әрекеттерді хаттамалау кезінде мынадай ақпарат жазылады:

1) иесінің идентификаторы (есептік жазба);

2) оқиға күні мен уақыты (күн форматы: КК: АА: ЖЖЖЖ, уақыт форматы: СС:ММ : СС);

3) оқиға дереккөзінің атауы (әрекет болған жүйенің компоненті немесе сервисі);

4) клиенттің немесе сессияның IP адресі;

5) оқиғаның сипаттамасы;

6) операцияның нәтижесі (сәттілік/сәтсіздік және код немесе істен шығу себебі).

14. Бұлтты сақтау қоймасының бағдарламалық-аппараттық қамтамасыз етілуі цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптарға сәйкес Қазақстан Республикасының аумағында орналастырылады.

15. Бұлтты ЭЦҚ жабық кілтін қорғау цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы біріңғай талаптарға сәйкес ұйымдастырушылық, бағдарламалық және техникалық іс-шаралар кешенімен қамтамасыз етіледі.

16. КО көп факторлы аутентификациясыз бұлтты ЭЦҚ жабық кілтін пайдаланумен электрондық құжаттарға қол қою мүмкіндігінің жоқтығын қамтамасыз етеді.