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 бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2020 жылғы 30 қазанда № 21549 болып тіркелді.

"Электрондық құжат және электрондық цифрлық қолтаңба туралы" 2003 жылғы 7 қаңтардағы Қазақстан Республикасы Заңының 5-бабы 1-тармағының 13-3) тармақшасына сәйкес БҰЙЫРАМЫН:

1. Қоса беріліп отырған Куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін жасау, пайдалану және сақтау қағидалары бекітілсін.

2. Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Мемлекеттік көрсетілетін қызметтер комитеті заңнамада белгіленген тәртіппен:

1) осы бұйрықты Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрықты ресми жарияланғаннан кейін Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің интернет-ресурсында орналастыруды;

3) осы бұйрық Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркеуден өткеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Заң департаментіне осы тармақтың 1) және 2) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтерді ұсынуды қамтамасыз етсін.

3. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі вице-министріне жүктелсін.

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

Қазақстан Республикасының
Цифрлық даму, инновациялар және
аэроғарыш өнеркәсібі министрі *Б. Мусин*

"КЕЛІСІЛДІ"
Қазақстан Республикасының
Сауда және интеграция министрлігі
"КЕЛІСІЛДІ"

Қазақстан Республикасының
Ұлттық қауіпсіздік комитеті

Қазақстан Республикасының
Цифрлық даму, инновациялар
және аэроғарыш өнеркәсібі
министрінің
2020 жылғы 27 қазаны
№ 405/НҚ бұйрығымен
бекітілген

Куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін жасау, пайдалану және сақтау қағидалары

1-тарау. Жалпы ережелер

1. Осы куәландырушы орталықта электрондық цифрлық қолтаңбаның жабық кілттерін жасау, сақтау және пайдалану қағидалары (бұдан әрі – Қағидалар) " Электрондық құжат және электрондық цифрлық қолтаңба туралы" Қазақстан Республикасының Заңына сәйкес әзірленді және бұлтты сервистерде электрондық цифрлық қолтаңбаның жабық кілттерін жасау, пайдалану және сақтау тәртібін айқындайды.

Ескерту. 1-тармақ жаңа редакцияда – ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 17.03.2023 № 95/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

2. Осы Қағидаларда мынадай ұғымдар қолданылады:

1) биометриялық сәйкестендіру – жеке басты физиологиялық және биологиялық өзгермейтін белгілері негізінде сәйкестендіретін шаралар кешені;

2) блокчейн – өзара байланысты деректер блоктарының, тұтастығын растаудың берілген алгоритмдері мен шифрлау құралдарының тізбектері базасында деректердің таратылған платформасындағы ақпараттың өзгермеуін қамтамасыз ететін ақпараттық-коммуникациялық технология;

3) көп факторлы сәйкестендіру – парольдерді немесе сәйкестендіру белгілерін (цифрлық сертификаттар, токендер, смарт-карталар, бір жолғы парольдердің генераторлары және биометриялық сәйкестендіруші құралдар) құру мен енгізуді қоса алғанда, түрлі параметрлер комбинациясының көмегімен пайдаланушының шынайылығын тексеру тәсілі;

4) куәландырушы орталық (бұдан әрі – КО) – электрондық цифрлық қолтаңбаның ашық кілтінің электрондық цифрлық қолтаңбаның жабық кілтіне сәйкестігін куәландыратын, сондай-ақ тіркеу куәлігінің анықтығын растайтын заңды тұлға;

5) тіркеу куәлігін иеленуші (бұдан әрі – иеленуші) – өз атына тіркеу куәлігі берілген , тіркеу куәлігінде көрсетілген ашық кілтке сәйкес келетін жабық кілтті құқыққа сыйымды иеленетін жеке немесе заңды тұлға;

6) электрондық цифрлық қолтаңба (бұдан әрі – ЭЦҚ) – электрондық цифрлық қолтаңба құралдарымен жасалған және электрондық құжаттың анықтығын, оның тиесілілігін және мазмұнының өзгермейтіндігін растайтын электрондық цифрлық нышандар жиынтығы;

7) ЭЦҚ ашық кілті – кез келген тұлғаға қолжетімді және электрондық құжаттағы электрондық цифрлық қолтаңбаның төлнұсқалығын растауға арналған электрондық цифрлық нышандар дәйектілігі;

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

9) ЭЦҚ құралдары – электрондық цифрлық қолтаңбаны жасау және оның төлнұсқалығын тексеру үшін пайдаланылатын бағдарламалық және техникалық құралдардың жиынтығы;

10) бұлтты ЭЦҚ – куәландырушы орталықтың HSM-де электрондық цифрлық қолтаңбаның жабық кілттерін жасауға, пайдалануға, сақтауға және жоюға мүмкіндік беретін сервисі, мұнда жеке кілтке қол жеткізуді иеленуші кемінде екі аутентификация факторы арқылы қашықтан жүзеге асырады, олардың бірі биометриялық болып табылады;

11) хэш – еркін ұзындықтағы кіріс деректерінің құрылымын белгіленген ұзындықтың бит-ке түрлендіру;

12) (Hardware Security Module) аппараттық криптографиялық модулі (бұдан әрі – HSM) – ақпаратты шифрлауға және ЭЦҚ ашық және жабық кілттерін басқаруға арналған аппараттық криптографиялық модуль.

Ескерту. 2-тармақ жаңа редакцияда – ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 17.03.2023 № 95/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

2-тарау. Куәландырушы орталықта ЭЦҚ жабық кілттерін жасау тәртібі

3. ЭЦҚ жабық кілттерін КО:

1) иеленушіге берілетін иеленушінің негізгі ақпаратын тасымалдаушыда;

2) бұлтты ЭЦҚ-да жасайды.

4. Бұлтты ЭЦҚ жабық кілттері қатаң түрде HSM ішінде жасалады. Жеке кілт HSM-ден ашық түрде алынбайды.

Бұл ретте HSM:

1) ҚР СТ 1073-2007 "Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар" стандартында белгіленген талаптарға сәйкес үшінші қауіпсіздік деңгейінен төмен емес;

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

3) Қазақстан Республикасының қолданыстағы заңнама талаптарына сәйкес ақпаратты және техникалық құралдарды қорғау тиімділігінің нормасын және олардың қорғалуын бағалау әдістемесіне сәйкес болады.

5. HSM-мен негізгі ақпаратты мұрағаттау тек шифрланған түрде және шифрлау кілтін N-ден M схемасы бойынша бөлу арқылы ғана мүмкін болады (5-тің 3-інен кем емес). N-ден M схемасы бойынша шифрлау кілттері қорғалған токендерде сақталады, Мемлекеттік КО арналған N төкен ақпараттандыру саласындағы уәкілетті органда, ұлттық қауіпсіздік органдарында және КО-да тұрақты сақталады. Қорғалған таңбалауыштар HSM резервтік мұрағатын қалпына келтіру кезінде ғана қолданылады.

6. ЭЦҚ жабық кілтін жасау және ЭЦҚ тіркеу куәлігін шығару алдында иеленуші дербес деректерді жинауға және өңдеуге келісім береді.

Иеленуші:

1) қашықтан, көп факторлы сәйкестендіруді қолдана отырып, әдістердің бірі биометриялық сәйкестендіру болып табылады;

2) КО тіркеу орталығында биометриялық сәйкестендіруді пайдалана отырып, қажет болған жағдайда биометриялық деректерді жинау рәсімінен сәйкестендіруден өтеді, КО биометриялық деректерді сақтауды қамтамасыз етеді.

Иеленуші бұлтты ЭЦҚ-да ЭЦҚ жабық кілтін сақтауға келісім береді.

7. ЭЦҚ жабық кілті жасалғаннан кейін МЕМСТ 28147-89 стандартын қолдана отырып, HSM-де шифрланған түрде сақталады. Құпия мәндер ретінде КО-да сақталмайтын иеленуші анықтаған пароль қатысады. КО иеленушінің жеке кілтінің құпия сөзін тексеру үшін HSM-де пароль хэшін сақтайды.

3-тарау. Куәландырушы орталықта сақталатын ЭЦҚ жабық кілттерін пайдалану тәртібі

8. КО-да сақталатын ЭЦҚ жабық кілттерін пайдалану кезінде иеленуші көп факторлы сәйкестендіруден өтеді, әдістердің бірі биометриялық сәйкестендіру болып табылады.

9. Электрондық құжаттарға қол қою HSM жадында қол қойылған файлды немесе оның хэшін HSM-ге беру арқылы жүзеге асырылады.

10. Иеленушіні КО-да сәйкестендіру кезінде иеленушіден парольді (браузер, мобильді қосымша) HSM-ге беру шифрланған түрде жүргізіледі, бұл ретте парольді шифрлау иеленушінің жағында, дербес компьютерде немесе смартфонда жүргізіледі.

11. Бұлтты ЭЦҚ-да ЭЦҚ жабық кілтінен парольді қалпына келтіру жүзеге асырылмайды.

12. КО иеленушіге бұлтты ЭЦҚ жабық кілтін, КО жеке кабинеті арқылы қол қойылған барлық электрондық құжаттар туралы ақпаратқа қол жеткізуді ұсынады.

Барлық қол қойылған электрондық құжаттар туралы ақпаратты сақтау мерзімі иеленушінің тіркеу куәлігінің қолданылу мерзімі өткеннен кейін кемінде бір жылды құрайды.

13. Тіркеу куәліктері иеленушілердің электрондық қолының жабық кілттерінің компрометациялау фактісі анықталған жағдайда, КО осы факті және келтірілген залалды барынша азайту бойынша қабылданған шаралар туралы ақпаратты өзінің интернет-ресурсында дереу жариялайды.

14. КО келесі оқиғалардың хаттамалануын қамтамасыз етеді:

1) бұлтты ЭЦҚ-мен ЭЦҚ жабық кілтін қалыптастыру;

2) бұлтты ЭЦҚ-мен ЭЦҚ жабық кілтін пайдалану;

3) бұлтты ЭЦҚ-мен ЭЦҚ жабық кілтін жою (өшіру).

Жұмыс хаттамаларын сақтау мерзімі тіркеу куәлігінің қолданылу мерзімі өткен күннен бастап бір жылды құрайды.

Іс-әрекеттерді хаттамалау кезінде мынадай ақпарат жазылады:

1) иеленуші идентификаторы;

2) күні, уақыты;

3) оқиға.

15. Оқиғалар хаттамалары күн сайын хэшке айналады және хэш деректері блокчейн оқиғалар тізбегінде сақталады. Бұл үшін қолданылатын блок Интернетте қол жетімді болады.

4-тарау. ЭЦҚ жабық кілттерін куәландырушы орталықта сақтау тәртібі

16. КО КО-дағы ЭЦҚ жабық кілттерін қорғауды қамтамасыз етеді.

17. ЭЦҚ жабық кілттерін бұлтты ЭЦҚ-да сақтау мерзімі Заңның 21-бабы 1-тармағының 2-1) тармақшасына сәйкес КО бекітетін КО тіркеу куәліктерін қолдану қағидаларында сипатталады.

18. Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптардың (бұдан әрі – БТ) 92-тармағына сәйкес бұлтты ЭЦҚ бағдарламалық-аппараттық қамтамасыз ету Қазақстан Республикасының аумағында орналастырылады.

19. Жабық кілттерді қорғау БТ-да сипатталған талаптарға сәйкес ұйымдастырушылық, бағдарламалық және техникалық іс-шаралар кешенімен қамтамасыз етіледі.

20. КО көп факторлы аутентификациясыз бұлтты ЭЦҚ ЭЦҚ жабық кілттерін пайдалана отырып, электрондық құжаттарға қол қою мүмкіндігінің болмауын қамтамасыз етеді.

Ескерту. 20-тармақ жаңа редакцияда – ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 17.03.2023 № 95/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

21. Осы Қағидалардың талаптарын орындау Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2020 жылғы 1 маусымдағы № 224/НҚ бұйрығымен бекітілген Куәландырушы орталықтарды аккредиттеуді жүргізу қағидаларына (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 20815 болып тіркелген) сәйкес КО аккредиттеу кезінде қажетті шарт болып табылады.