Электрондық цифрлық қолтаңбаның төлнұсқалығын тексеру қағидаларын бекіту туралы

Қазақстан Республикасы Инвестициялар және даму министрінің 2015 жылғы 9 желтоқсандағы № 1187 бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2016 жылы 14 қаңтарда № 12864 болып тіркелді.

"Электрондық құжат және электрондық цифрлық қолтаңба туралы"
2003 жылғы 7 қаңтардағы Қазақстан Республикасы Заңының
5-бабының 1-тармағы 10) тармақшасына сәйкес, **БҰЙЫРАМЫН:**

1. Қоса беріліп отырған Электрондық цифрлық қолтаңбаның төлнұсқалығын тексеру қағидалары бекітілсін.

2. Қазақстан Республикасы Инвестициялар және даму министрлігінің Байланыс, ақпараттандыру және ақпарат комитеті (Т.Б. Қазанғап):

1) осы бұйрықтың Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркелуін;

2) осы бұйрық Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркелгеннен кейін күнтізбелік он күн ішінде мерзімді баспа басылымдарында және " Әділет" ақпараттық-құқықтық жүйесінде, сондай-ақ Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкіне енгізу үшін Республикалық құқықтық ақпарат орталығына ресми жариялауға оның көшірмелерін баспа және электронды түрде жіберуді;

3) осы бұйрықты Қазақстан Республикасы Инвестициялар және даму министрлігінің интернет-ресурсында және мемлекеттік органдардың интранет-порталында орналастыруды;

1) осы бұйрық Қазақстан Республикасы Әділет министрлігінде мемлекетік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Инвестициялар және даму министрлігінің Заң департаментіне осы бұйрықтың 2-тармағының 1), 2) және 3) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтерді ұсынуды қамтамасыз етсін.

3. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Инвестициялар және даму вице-министріне жүктелсін.

4. Осы бұйрық оның алғышқы ресми жарияланған күнінен бастап қолданысқа енгізіледі және 2016 жылғы 1 қаңтардан бастап туындаған құқықтық қатынастарға қолданылады.

Қазақстан Республикасының
Инвестициялар және даму
министрі Ә. Исекешев

Қазақстан Республикасы
Инвестициялар және даму министрінің
2015 жылғы 9 желтоқсандағы
№ 1187 бұйрығымен
бекітілген

Электрондық цифрлық қолтаңбаның түпнұсқалығын тексеру қағидалары

Ескерту. Қағида жаңа редакцияда – ҚР Ақпарат және коммуникациялар министрінің 30.12.2016 № 316 (алғашқы ресми жарияланған күнінен бастап күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

1-тарау. Жалпы ережелер

1. Осы Электрондық цифрлық қолтаңбаның түпнұсқалығын тексеру қағидалары (бұдан әрі – Қағидалар) "Электрондық құжат және электрондық цифрлық қолтаңба туралы" 2003 жылғы 7 қаңтардағы Қазақстан Республикасының Заңы (бұдан әрі – Заң) 5-бабының 10) тармақшасына сәйкес әзірленді және ақпараттық жүйені құру мен жұмыс істеуі кезеңінде ақпараттық жүйенің электрондық цифрлық қолтаңбаның түпнұсқалығын тексеру тәртібін айқындайды.

2. Осы Қағидаларда мынадай ұғымдар пайдаланылады:

1) ақпаратты криптографиялық қорғау құралы (бұдан әрі – АККҚ) – криптографиялық түрлендіру алгоритмдерін, кілттерді өндіруді, қалыптастыруды, бөлуді және басқаруды жүзеге асыратын құрал;

2) кері қайтарып алынған тіркеу куәліктерінің тізімі (бұдан әрі – КТКТ) – әрекеті тоқтатылған тіркеу куәліктері, олардың сериялық нөмірлері, кері қайтару (жою) себебі мерзімі және туралы мәліметтер қамтылған тіркеу куәліктері тіркелімінің бөлігі;

3) куәландырушы орталық – электрондық цифрлық қолтаңба ашық кілтінің электрондық цифрлық қолтаңбаның жабық кілтіне сәйкестігін куәландыратын, сондай-ақ тіркеу куәлігінің дұрыстығын растайтын заңды тұлға;

4) тіркеу куәлігі – электрондық цифрлық қолтаңбаның Заңмен белгіленген талаптарға сәйкестігін растау үшін куәландырушы орталық беретін қағаз тасығыштағы құжат немесе электрондық құжат;

5) электрондық құжат – өзіндегі ақпарат электрондық-цифрлық нысанда ұсынылған және электрондық цифрлық қолтаңба арқылы куәландырылған құжат;

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

7) ЭЦҚ құралдары – электрондық цифрлық қолтаңбаны жасау және түпнұсқалығын тексеру үшін пайдаланылатын бағдарламалық және техникалық құралдардың жиынтығы;

8) еркін ұзындығымен кіріс деректердің массивін ұзындығы тіркелген биталық жағына хэш-түрлендіру;

9) хэш-функция – байт реттілігін тіркелген өлшемдегі байт реттілігінде бейнелеу функциясы.

2-тарау. Электрондық цифрлық қолтаңбаның түпнұсқалығын тексеру тәртібі

3. Ақпараттық жүйені құру мен жұмыс істеуі кезеңінде қол қоюшы тараптың тіркеу куәлігін қамтитын электрондық құжатты алған кезде ақпараттық жүйеде мына тексерулерді жүзеге асыратын ЭЦҚ түпнұсқалығын тексеру функционалы іске асырылады:

1) электрондық құжаттағы ЭЦҚ тексеру;

2) қол қоюшы тараптың тіркеу куәлігін тексеру.

4. Ақпараттық жүйе электрондық құжаттағы ЭЦҚ-ны қол қоюшы тараптың тіркеу куәлігіндегі ЭЦҚ ашық кілтін пайдалану арқылы тексереді. Электрондық құжатта қол қоюшы тараптың тіркеу куәлігі болуға тиіс.

5. ЭЦҚ-ны тексеру құжатқа қол қойылған тәртіптің кері тәртібімен мынадай схема бойынша жүзеге асырылады:

1) жөнелтушінің ЭЦҚ ашық кілтінің көмегімен хабарлама хэшінің (жіберушінің қолы) мәні ашылады;

2) хэш – функциясының көмегімен түпнұсқалық хабарламаның бақылау сомасы есептеледі.

Екі бақылау соманы салыстыру жүргізіледі, егер олар тең болса, ЭЦҚ дұрыс (ЭЦҚ тексерудің жағымды нәтижесі айқындалды) болып есептеледі, егер тең болмаса, ЭЦҚ дұрыс емес (ЭЦҚ тексерудің жағымсыз нәтижесі айқындалды) болып есептеледі.

6. ЭЦҚ тексерудің жағымды нәтижесі анықталған жағдайда, ақпараттық жүйе АККҚ мен куәландырушы орталықтың ЭЦҚ құралдарын пайдалана отырып, мынадай тексерулерді орындау арқылы қол қоюшы тараптың тіркеу куәліктерін тексереді:

1) тіркеу куәлігінің жарамдылық мерзімін тексеру. Куәландырушы орталықтардың аралық тіркеу куәліктерін ескере отырып, тексерілетін тіркеу куәлігінен куәландырушы орталығының сенім білдірілген негізгі тіркеу куәлігіне дейін қолданыс мерзімдерін тексеру;

2) тіркеу куәлігін кері қайтаруға (жоюға) қатысты тексеру. Тіркеу куәлігін кері қайтарылуға (жойюға) қатысты тексеру мынадай әдістердің бірімен жүзеге асырылады:

куәландырушы орталықтың ҚТКТ негізінде. Осы тексеру әдісі тексеріліп отырған тіркеу куәлігі куәландырушы орталығының ҚТКТ қолдану мерзімі басталған сәттен жойылғандығын растайды;

On-line Certificate Status Protocol (бұдан әрі – OCSP) хаттамасына негізделген тіркеу куәлігінің жойылғандығына қатысты онлайн тексеру. Осы тексеру әдісі тексеріліп отырған тіркеу куәлігі OCSP түбіртегінде қалыптастырылған сәтінде жойылғандығын растайды;

қосымша ҚТКТ негізінде. Аталған сервис ҚТКТ сервисімен бірге пайдаланады, бұл ҚТКТ сервисіне қарағанда барынша өзектілендірілген ақпаратты алуға мүмкіндік береді. Осы тексеру әдісі тексеріліп отырған тіркеу куәлігі куәландырушы орталығының қосымша ҚТКТ қолдану мерзімі басталған сәттен жойылғандығын растайды;

3) тіркеу куәлігінің ЭЦҚ пайдалану саласын тексеру. Тексеру "кілтті пайдалану" (KeyUsage) тіркеу куәлігі жолының мәнін тексеруді қамтиды. "Кілтті пайдалану" өрісі қамтитын "Цифрлық қолтаңба" мен "Бастартпаушылық" мәндері тіркеу куәлігі ЭЦҚ үшін пайдаланылатынын білдіреді. "Кілтті пайдалану" жолы "Цифрлық қолтаңба" мен "Кілттерді шифрлау" мәндері бұл тіркеу куәлігі аутентификация үшін пайдаланылатынын білдіреді;

4) тіркеу куәлігі саясатының нөмірін және оны пайдаланудың рұқсат етілген әдістерін тексеру. Тексеріліп отырған тіркеу куәлігінің саясаты тіркеу куәлігін пайдаланудың рұқсат етілген және тыйым салынған әдістерін қамтиды (мәселен: тіркеу куәлігі "Қазынашылық-клиент" ақпараттық жүйесінде пайдаланылады), бұл осы тіркеу куәлігін "Қазынашылық-клиент" ақпараттық жүйесінен басқа ақпараттық жүйелерде пайдалануға жол берілмейтінін білдіреді;

5) куәландырушы орталықтардың аралық тіркеу куәліктерін ескере отырып, куәландырушы орталықтың тексеріліп отырған тіркеу куәлігінен негізгі сенім білдірілген тіркеу куәлігіне дейінгі дұрыс тізбектің құрылуын тексеру;

6) уақыт белгісін тексеру. Уақыт белгісінің түбіртегін тексеру ұзақ мерзім сақталатын электрондық құжаттар үшін жүргізіледі. Уақыт белгісінің түбіртегі ЭЦҚ тексерудің жағымды нәтижесі анықталған кезде электрондық құжатқа қол қойылған сәтте қалыптастырылып, уақыттың көрсетілген кезеңінде құжатқа қол қоюдың дәлелі болып табылады.

Уақыт белгісі түбіртекте көрсетілген уақытта ЭЦҚ болғанының дәлелі болып табылады;

7) құжатқа қол қойған тұлғаның өкілеттігін тексеру. Өкілеттіктерді тексеру механизмдерін ақпараттық жүйе жүзеге асырады. Өкілеттіктерді тексеру тіркеу куәлігінде бұл туралы ақпарат қамтылған кезде жүзеге асырылады.

Осы тармақтың 6) және 7) тармақшаларын қоспағанда, ЭЦҚ немесе тіркеу куәлігі жоғарыда аталған тексерулердің ең болмаса біреуінің талаптарына сәйкес келмеген

кезде ЭЦҚ немесе тіркеу куәлігі жарамсыз (ЭЦҚ және тіркеу куәлігін тексрудің жағымсыз нәтижесі айқындалды) болып есептеледі.

7. ЭЦҚ мен тіркеу куәлігінің түпнұсқалығын тексеруді техникалық іске асыру ақпараттық жүйеге жүктеледі.

8. ЭЦҚ тексеру процедурасын жүргізгеннен кейін КО АКҚҚ пайдалана отырып ЭЦҚ түпнұсқалығын растау (белгілеу) кезінде (ЭЦҚ және тіркеу куәлігін тексерудің жағымды нәтижесі айқындалды), сондай-ақ Заңның 10-бабы 1-тармағының 2), 3) және 4) тармақшалары бойынша шарттарға сәйкес келген кезде ақпараттық жүйе арқылы алынған электрондық құжат бірдей құқықтық салдарымен жеке қол қойылған құжатқа тең болып танылады.

9. АКҚҚ пайдалана отырып, ЭЦҚ түпнұсқалығын тексеру процедурасын жүргізгеннен кейін ЭЦҚ сәйкессіздігі (ЭЦҚ тексерудің жағымсыз нәтижесі айқындалды) айқындалған кезде, сондай-ақ Заңның 10-бабы 1-тармағының 2), 3) және 4) тармақшалары бойынша шарттарға сәйкес келмеген кезде ақпараттық жүйе арқылы алынған электрондық құжат жеке қол қойылған құжатқа тең болып танылмайды.