Электрондық цифрлық қолтаңбаны қалыптастыру және оның түпнұсқалығын тексеру қағидаларын бекіту туралы

Қазақстан Республикасы Премьер-Министрінің орынбасары – Жасанды интеллект және цифрлық даму министрінің 2026 жылғы 21 тамыздағы № 500/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2026 жылғы 24 тамызда № 39672 болып тіркелді

Қазақстан Республикасы Цифрлық кодексінің 55-бабы 1-тармағының 4) тармақшасына сәйкес БҰЙЫРАМЫН:

1. Қоса беріліп отырған электрондық цифрлық қолтаңбаны қалыптастыру және оның түпнұсқалығын тексеру қағидалары бекітілсін.

2. Мыналардың күші жойылды деп танылсын:

1) "Электрондық цифрлық қолтаңбаның төлнұсқалығын тексеру қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің 2015 жылғы 9 желтоқсандағы № 1187 бұйрығының (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 12864 болып тіркелген);

2) "Электрондық цифрлық қолтаңбаның төлнұсқалығын тексеру қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің 2015 жылғы 9 желтоқсандағы № 1187 бұйрығына өзгеріс енгізу туралы" Қазақстан Республикасы Ақпарат және коммуникациялар министрінің 2016 жылғы 30 желтоқсандағы № 316 б ұйрығының (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 14759 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*

Қазақстан Республикасы
Премьер-Министрінің
орынбасары – Жасанды
интеллект және
цифрлық даму министрі
2026 жылғы 21 тамыздағы
№ 500/НҚ бұйрықпен
бекітілген

Электрондық цифрлық қолтаңбаны қалыптастыру және оның түпнұсқалығын тексеру қағидалары

1-тарау. Жалпы ережелер

1. Осы Электрондық цифрлық қолтаңбаны қалыптастыру және оның түпнұсқалығын тексеру қағидалары (бұдан әрі – Қағидалар) Қазақстан Республикасы Цифрлық кодексінің (бұдан әрі – Кодекс) 55-бабы 1-тармағының 4) тармақшасына сәйкес әзірленді және электрондық құжатта электрондық цифрлық қолтаңбаны қалыптастыру мен оның түпнұсқалығын тексерудің тәртібін белгілейді.

2. Осы Қағидаларда мынадай ұғымдар қолданылады:

1) кері қайтарып алынған электрондық цифрлық қолтаңба ашық кілті сертификаттарының тізімі сервисі – RFC 5280 талаптарына сәйкес қалыптастырылған кері қайтарып алынған электрондық цифрлық қолтаңбаның ашық кілті сертификаттарының тізімін ұсынатын сервис;

2) куәландырушы орталық – Қазақстан Республикасының заңнамасына сәйкес құрылған, электрондық цифрлық қолтаңбаның ашық кілттері сертификаттарының анықтығын, электрондық цифрлық қолтаңбаның ашық кілттерінің тиесілілігін және жарамдылығын растайтын заңды тұлға;

3) объектілік сәйкестендіргіш (бұдан әрі – OID) – цифрлық объектіге халықаралық объектілік сәйкестендіргіш тармағында оны бірмәнді сәйкестендіру үшін берілетін бірегей иерархиялық сандық сәйкестендіргіш тізбегі;

4) сертификаттың иегері – атына электрондық цифрлық қолтаңбаның ашық кілті сертификаты берілген, электрондық цифрлық қолтаңбаның ашық кілті сертификатында көрсетілген ашық кілтке сәйкес келетін жабық кілтті заңды түрде иеленетін жеке немесе заңды тұлға;

5) уақыт белгісінің сервисі – RFC 3161 және RFC 5816 талаптарына сәйкес уақыт белгісі түбіртегін қалыптастыру сәтінде электрондық құжатта электрондық цифрлық

қолтаңбаның болғанын растайтын уақыт белгісінің түбіртегін ұсынатын куәландырушы орталықтың онлайн-сервисі;

6) хэш – деректерден алынатын және олардың тұтастығын тексеру үшін қолданылатын тіркелген ұзындықтағы мән;

7) цифрлық жүйе – цифрлық деректерді құруды, жинауды, өңдеуді, сақтауды және таратуды қамтамасыз ету мақсатында цифрлық инфрақұрылым объектілерін пайдаланатын, сондай-ақ цифрлық орта субъектілерінің өзара іс-қимылын автоматтандыратын және (немесе) цифрлық ортада қызметтер көрсетуді қамтамасыз ететін функционалдық байланысты цифрлық ресурстар кешені;

8) электрондық құжат – анықтығы, тиесілігі және өзгермейтіндігін растау электрондық цифрлық қолтаңбаның көмегімен қамтамасыз етілген цифрлық жазба;

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

10) электрондық цифрлық қолтаңбаның ашық кілті сертификаты (бұдан әрі – сертификат) – куәландырушы орталықтың электрондық цифрлық қолтаңбасымен куәландырылған, электрондық цифрлық қолтаңбаның осы Кодексте белгіленген талаптарға сәйкестігін растауды жүзеге асыратын цифрлық жазба;

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

12) электрондық цифрлық қолтаңбаның ашық кілті сертификатының мәртебесін тексеру сервисі (Online Certificate Status Protocol, бұдан әрі – OCSP) – RFC 6960 талаптарына сәйкес берілген OCSP-түбіртегі берілген сәтте электрондық цифрлық қолтаңбаның ашық кілті сертификатының кері қайтарып алынғаны туралы мәліметтерді не мұндай кері қайтарып алудың жоқ екендігі туралы мәліметтерді қамтитын OCSP-түбіртегін ұсынатын куәландырушы орталықтың онлайн-сервисі;

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

14) CAdES форматы (CMS Advanced Electronic Signatures, бұдан әрі – CAdES) – CMS негізіндегі электрондық цифрлық қолтаңба форматы;

15) CMS форматы (Cryptographic Message Syntax, бұдан әрі – CMS) –электрондық цифрлық қолтаңбаны қалыптастыру және тексеру үшін қолданылатын криптографиялық хабарлама форматы;

16) PAdES форматы (PDF Advanced Electronic Signatures, бұдан әрі – PAdES) – PDF форматындағы құжаттарға арналған электрондық цифрлық қолтаңба форматы;

17) PDF форматы (Portable Document Format, бұдан әрі – PDF) – электрондық цифрлық қолтаңбаны ендіріліп орналастыруды қолдайтын электрондық құжат форматы ;

18) X.509 стандарты – электрондық цифрлық қолтаңбаның ашық кілті сертификаты көмегімен ашық кілттерді тарату рәсімдері мен деректер форматтарын айқындайтын стандарт;

19) XAdES форматы (XML Advanced Electronic Signatures, бұдан әрі – XAdES) – XML форматындағы құжаттарға арналған электрондық цифрлық қолтаңба форматы;

20) XML кеңейтілетін белгілеу тілі (eXtensible Markup Language, бұдан әрі – XML) – деректерді құрылымдық және машина оқитын сақтау және беру үшін пайдаланылатын кеңейтілетін белгілеу тілі.

2-тарау. Электрондық цифрлық қолтаңбаны қалыптастыру және оның түпнұсқалығын тексеру

1-параграф. Электрондық цифрлық қолтаңбаны қалыптастыру

3. ЭЦҚ қалыптастыру ЭЦҚ-ның жабық кілтін пайдалана отырып, сертификат иегерімен не цифрлық жүйе арқылы жүзеге асырылады.

4. ЭЦҚ қалыптастыру алдында қол қоюшы тұлғаның сертификатына қатысты мынадай тексерулер:

1) куәландырушы орталықтың ЭЦҚ тексеру жолымен сертификаттың түпнұсқалығын криптографиялық тексеру;

2) сертификаттың қолданылу мерзімінің басталғанын және аяқталмағанын анықтай отырып, оның қолданылу мерзімін тексеру;

3) OCSP онлайн-сервисі арқылы, ал ол қолжетімсіз болған жағдайда кері қайтарылып алынған сертификаттар тізімі сервисі арқылы сертификаттың кері қайтарылып алынған туралы мәліметтердің жоқтығын тексеру жүзеге асырылады. Кері қайтарылып алынған сертификаттар тізімі сервисін пайдалану кезінде кері қайтарылып алынған сертификаттардың өзекті тізімі (Certificate Revocation List, бұдан әрі – CRL) және кері қайтарылып алынған сертификаттардың аралық тізімі (Delta Certificate Revocation List, бұдан әрі – delta CRL) қолданылады. Delta CRL пайдалану міндетті болып табылмайды және CRL қолданылу кезеңінде сертификаттың кері қайтарылуы туралы мәліметті нақтылау үшін қолданылады;

4) куәландырушы орталықтың сертификаттарды қолдану саясатына сәйкес сертификатты қолдану саласы мен мақсаттарын тексеру жүзеге асырылады.

5. ЭЦҚ қалыптастырылған уақытын растау немесе сертификаттың қолданылу мерзімі аяқталғаннан не ол кері қайтарып алынғаннан кейін ЭЦҚ тексеру талап етілетін құжаттар үшін ЭЦҚ қалыптастырылған күні мен уақыты ретінде уақыт белгісінің түбіртегінде көрсетілген күн мен уақыт танылады. ЭЦҚ қалыптастырылған сәтті растау

үшін уақыт белгісінің туралы түбіртегі ЭЦҚ қалыптастырылғаннан кейін тікелей қалыптастырылады.

6. Уақыт белгісінің түбіртегі болмаған жағдайда ЭЦҚ қалыптастырылған күн мен уақытты анық түрде айқындау мүмкін емес.

7. ЭЦҚ қалыптастыру үшін мынадай:

1) CAdES – кез келген форматтағы құжаттарға арналған (PKCS#7-пен үйлесімді CMS негізінде);

2) PAdES – PDF форматындағы құжаттарға арналған;

3) XAdES – құрылымдалған XML-құжаттарға арналған негізгі форматтар қолданылады.

Осы Қағидаларға сәйкес ЭЦҚ тексеру мүмкіндігі қамтамасыз етілген жағдайда ЭЦҚ-ның өзге форматтарын қолдануға жол беріледі.

8. CAdES форматы мыналарды қамтиды:

1) құрылымдық элементтер:

қол қойылатын деректерді бірмәнді белгілеуге мүмкіндік беретін қол қойылатын деректер не олардың хэші;

ЭЦҚ мәні;

ЭЦҚ қалыптастыру алгоритмі;

қол қоюшы тұлғаның сертификаты;

"messageDigest" атрибуты (OID: 1.2.840.113549.1.9.4) – қол қойылатын деректердің хэшін қамтиды;

"signingCertificateV2" атрибуты (OID: 1.2.840.113549.1.9.16.2.47) – қолтаңбаны қалыптастыру кезінде пайдаланылған қол қоюшы тұлға сертификатының хэшін қамтиды;

"contentType" атрибуты (OID: 1.2.840.113549.1.9.3) – қол қойылатын деректердің типін айқындайды.

2) қосымша (опционалды) құрылымдық элементтер:

уақыт белгісінің түбіртегі (OID: 1.2.840.113549.1.9.16.2.14) – уақыт белгісі сервисі қалыптастырған күнді және уақытты қамтиды, ЭЦҚ қалыптастырылған сәтті растайды;

сертификаттың кері қайтарып алынғаны туралы мәлімет (OID: 1.2.840.113549.1.9.16.2.24) – OCSP-түбіртегі не CRL;

сертификаттау тізбегінің сертификаттары (OID: 1.2.840.113549.1.9.16.2.23) – тексерілетін сертификаттан куәландырушы орталықтың сенімді негізгі сертификатына дейінгі сертификаттау тізбегін аралық сертификаттарды ескере отырып құруға және тексеруге қажетті сертификаттарды қамтиды;

өзге атрибуттар – оларды пайдалану ЭЦҚ-ны тексеруге кедергі келтірмеген жағдайда қалыптастырушы тараптың қалауы бойынша енгізілуі мүмкін.

9. PAdES форматы мыналарды қамтиды:

1) құрылымдық элементтерді:

қол қойылатын құжат;

қол қоюшы тұлғаның сертификаты;

"ByteRange" жазбасы – қол қойылатын құжаттың байттар диапазондарын айқындайды;

"SubFilter" жазбасы – CAdES ЭЦҚ форматының пайдаланылуын айқындайды;

"Contents" жазбасы – ЭЦҚ мәнін қамтиды.

2) PAdES форматындағы ЭЦҚ-ның қосымша (опционалды) құрылымдық элементтері осы Қағидалардың 9-тармағына сәйкес атрибуттарды қамтиды.

10. XAdES форматы мыналарды қамтиды:

1) құрылымдық элементтер:

қол қойылатын құжат;

"SignedInfo" элементі – қол қойылатын деректердің канондық ұсынылымын, оның ішінде оларға сілтемелерді, олардың хэшін және қолданылатын алгоритмдер туралы мәліметтерді қамтиды;

"SignatureValue" элементі – ЭЦҚ мәнін қамтиды;

"KeyInfo" элементі – қол қоюшы тұлғаның сертификатын не оны бірмәнді сәйкестендіруге және алуға арналған мәліметтерді қамтиды;

"SignedProperties" элементі – ЭЦҚ-ның қол қойылатын қасиеттерін қамтиды.

2) қосымша (опционалды) құрылымдық элементтер:

уақыт белгісінің түбіртегі – уақыт белгісінің сервисі қалыптастырған күнді және уақытты қамтиды, ЭЦҚ-ның қалыптастырылған сәтін растайды;

сертификаттың кері қайтарылып алынғаны туралы мәліметтер – OCSP-түбіртегі не CRL;

өзге элементтер мен атрибуттар – оларды пайдалану ЭЦҚ-ны тексеруге кедергі келтірмеген жағдайда қалыптастырушы тараптың қалауы бойынша енгізілуі мүмкін.

11. Электрондық құжатқа қол қою кезінде бір немесе бірнеше ЭЦҚ-ны пайдалануға жол беріледі.

12. Электрондық құжатта бір немесе бірнеше ЭЦҚ болуына жол беріледі. Әрбір кейінгі ЭЦҚ-ны қосу бұрын қалыптастырылған ЭЦҚ-ларды тексеру мүмкіндігін сақтай отырып, тиісті ЭЦҚ форматында көзделген тәсілмен жүзеге асырылады.

2-параграф. Электрондық цифрлық қолтаңбаның түпнұсқалығын тексеру

13. Электрондық құжаттағы ЭЦҚ-ны тексеру үшін қажетті деректер:

1) электрондық құжат не оның хэші;

2) электрондық құжаттың ЭЦҚ-сы;

3) қол қоюшы тұлғаның сертификаты;

4) қол қоюшы тұлғаның сертификатын берген куәландырушы орталықтың сертификаты, сондай-ақ куәландырушы орталықтың сенімді негізгі сертификатына дейінгі куәландырушы орталықтардың аралық сертификаттары;

5) уақыт белгісінің түбіртегі – опционалды;

6) қол қоюшы тұлғаның сертификатын берген куәландырушы орталықтың OCSP-түбіртегі не CRL (delta CRL болған жағдайда).

14. ЭЦҚ-ның түпнұсқалығын тексеру мыналарды:

1) электрондық құжатта ЭЦҚ-ны криптографиялық тексеруді;

2) қол қоюшы тұлғаның сертификатын тексеруді;

3) уақыт белгісінің түбіртегін тексеруді (бар болса) қамтиды.

Уақыт белгісінің түбіртегі болмаған кезде ЭЦҚ-ның түпнұсқалығын тексеру ЭЦҚ-ны тексеру сәтінде жүзеге асырылады. Уақыт белгісінің жарамды түбіртегі болған кезде ЭЦҚ-ның түпнұсқалығын тексеру уақыт белгісінің түбіртегінде көрсетілген уақыт сәтінде жүзеге асырылады.

15. ЭЦҚ-ны криптографиялық тексеру тексерілетін деректердің хэш мәнін тиісті сертификаттағы ЭЦҚ ашық кілтін пайдалана отырып, ЭЦҚ-ны тексеру алгоритмін орындау нәтижесімен салыстыру арқылы жүзеге асырылады.

Электрондық құжатта ЭЦҚ-ны тексеру қол қоюшы тұлғаның сертификатындағы ЭЦҚ-ның ашық кілтін пайдалана отырып жүзеге асырылады. Электрондық құжат әрбір қол қоюшы тұлғаның сертификатын қамтиды не оны алу мүмкіндігін қамтамасыз етеді. Көрсетілген сертификаттың болмауы ЭЦҚ-ны тексеру мүмкіндігін болдырмайды.

ЭЦҚ-ны криптографиялық тексеру нәтижесінің тексерілетін деректердің хэш мәніне сәйкес келмеуі ЭЦҚ-ның түпнұсқалығын тексерудің теріс нәтижесін білдіреді.

16. Қол қоюшы тұлғаның сертификатын тексеру ақпаратты криптографиялық қорғау құралдарын пайдаланумен жүзеге асырылады және мыналарды:

1) аралық сертификаттарды ескере отырып, тексерілетін сертификаттан куәландырушы орталықтың сенімді негізгі сертификатына дейін сертификаттау тізбегіндегі барлық сертификаттарды қоса алғанда, ЭЦҚ-ның түпнұсқалығын тексеру сәтінде сертификаттың қолданылу мерзімін тексеруді қамтиды. ЭЦҚ-ның түпнұсқалығын тексеру сәтінде сертификаттау тізбегінде кемінде бір сертификаттың қолданылу мерзімінің аяқталуы тексерудің теріс нәтижесін білдіреді;

2) осы Қағидалардың 18 және 19-тармақтарына сәйкес OCSP сервисі не CRL (delta CRL болған жағдайда) арқылы сертификаттың кері қайтарып алынғаны туралы мәліметтің жоқтығын тексеруді қамтиды. Сертификаттың кері қайтарып алынғаны туралы мәліметтің болуы тексерудің теріс нәтижесін білдіреді;

3) қол қоюшы тұлғаның сертификатынан куәландырушы орталықтың сенімді негізгі сертификатына дейінгі сертификаттау тізбегінің, оның ішінде куәландырушы орталықтардың аралық сертификаттарын қоса алғанда, дұрыс құрылуын тексеруді қамтиды. Сертификаттау тізбегінің дұрыс құрылмауы тексерудің теріс нәтижесін білдіреді;

4) сертификатты қолдану саясатына сәйкес тиісті куәландырушы орталықтың сертификаттарды қолдану саясатында белгіленген сертификатты пайдалану

шарттарына сертификат саясатының нөмірі мен Key Usage және Extended Key Usage кеңейтімдерімен айқындалатын кілт мақсатының сәйкестігін тексеруді қамтиды.

Осы тармақта көзделген тексерулердің кем дегенде біреуінің теріс нәтижесі ЭЦҚ түпнұсқалығын тексерудің теріс нәтижесін білдіреді.

17. Уақыт белгісінің түбіртегін тексеру мыналарды:

1) осы Қағидалардың 15 және 16-тармақтарына сәйкес уақыт белгісінің түбіртегінің ЭЦҚ түпнұсқалығын тексеруді;

2) уақыт белгісінің сервисін не уақыт белгісінің қалыптастырған және оған қол қойған куәландырушы орталықты айқындауға мүмкіндік беретін мәліметтердің болуын , сондай-ақ уақыт белгісі сервисінің сертификаты тексерілетін сертификатты берген куәландырушы орталықпен берілгенін растауды тексеруді;

3) уақыт белгісінің түбіртектерін қалыптастыруға арналған (timeStamping) кілт мақсатының уақыт белгісі сервисі сертификатында болуын тексеруді;

4) уақыт белгісі түбіртегінде қамтылған хэш мәнінің ЭЦҚ-ның қалыптастырылған деректерінің хэш мәніне сәйкестігіне қатысты тексеруді қамтиды.

Уақыт белгісінің түбіртегі осы тармақта көзделген барлық тексерулердің нәтижелері бойынша жарамды деп танылады. Уақыт белгісінің түбіртегін тексерудің теріс нәтижесі ЭЦҚ түпнұсқалығын тексерудің теріс нәтижесін білдіреді.

18. CRL және delta CRL-ды (бар болса) тексеру мыналарды:

1) CRL құрылымының X.509 форматына сәйкестігін, ASN.1/DER-кодтаудың дұрыстығын тексеруді;

2) CRL-ды қалыптастырған және оған қол қойған куәландырушы орталықты айқындауға мүмкіндік беретін мәліметтің болуын тексеруді;

3) CRL-дың тексерілетін сертификатқа сәйкестігін, CRL-дың тексерілетін сертификатты берген куәландырушы орталықпен қалыптастырылғанын анықтау арқылы тексеруді;

4) тиісті CRL-ның шығарған куәландырушы орталықтың сертификатында қамтылған ЭЦҚ ашық кілтін пайдалана отырып, CRL қол қойылатын деректерінің (TBSCertList) хэш мәнін CRL ЭЦҚ-ны тексеру алгоритмін орындау нәтижесімен салыстыру арқылы CRL ЭЦҚ-сына криптографиялық тексеру жүргізуді қамтиды. CRL ЭЦҚ-сына криптографиялық тексеру нәтижесінің CRL қол қойылатын деректерінің хэш мәніне сәйкес келмеуі CRL-ді тексерудің теріс нәтижесін білдіреді;

5) ЭЦҚ түпнұсқалығын тексеру сәтінде CRL немесе delta CRL қолданылу кезеңін тексеруді қамтиды. ЭЦҚ түпнұсқалығын тексеру сәтінде CRL немесе delta CRL қолданылу кезеңінің аяқталуы тексерудің теріс нәтижесін білдіреді.

Осы тармақта көзделген барлық тексерулердің оң нәтижесі болған кезде CRL немесе delta CRL тексеру нәтижесі оң болып табылады. Теріс нәтиже болған кезде, көрсетілген тексерулердің кем дегенде біреуі CRL немесе Delta CRL тексеру нәтижесі теріс болады.

19. OCSP-түбіртегін тексеру мыналарды:

1) OCSP-түбіртегі құрылымының OCSP стандарты талаптарына сәйкестігін, ASN.1/ DER-кодтаудың дұрыстығын тексеруді;

2) OCSP-түбіртегін қалыптастырған және оған қол қойған OCSP сервисін немесе куәландырушы орталықты айқындауға мүмкіндік беретін мәліметтердің болуын, сондай-ақ OCSP сервисінің сертификаты тексерілетін сертификатты берген куәландырушы орталықпен берілгенін растауды тексеруді;

3) OCSP-түбіртегіндегі сертификат сәйкестендіргіштерін тексерілетін сертификат деректерімен салыстыру арқылы OCSP-түбіртегінің тексерілетін сертификатқа сәйкестігін тексеруді;

4) OCSP-түбіртегіне қол қойған OCSP сервисінің немесе куәландырушы орталықтың сертификатында қамтылған ЭЦҚ-ның ашық кілтін пайдалана отырып, OCSP-түбіртегінің қол қойылатын деректерінің хэш мәнін OCSP-түбіртегінің ЭЦҚ-сын тексеру алгоритмін орындау нәтижесімен салыстыру арқылы OCSP-түбіртегінің ЭЦҚ-сына криптографиялық тексеру жүргізуді қамтиды. OCSP-түбіртегінің ЭЦҚ-сына криптографиялық тексеру нәтижесінің OCSP-түбіртегінің қол қойылатын деректерінің хэш мәніне сәйкес келмеуі OCSP-түбіртегін тексерудің теріс нәтижесін білдіреді;

5) OCSP-түбіртектеріне қол қоюға арналған (OCSPSigning) кілт мақсатының OCSP сервисінің немесе куәландырушы орталықтың сертификатында болуын тексеруді;

6) OCSP-түбіртекті (thisUpdate) беру сәті ЭЦҚ-ның түпнұсқалығын тексеру сәтінен бұрын болмайтынын тексеруді қамтиды. OCSP түбіртегіндегі мәртебе тексерілетін сертификаттың жай-күйін тек оны ұсынған кезде ғана сипаттайды және уақыттың басқа сәттеріне қолданылмайды;

7) тексерілетін сертификат үшін OCSP түбіртегіндегі "good" мәртебесінің болуын тексеруді қамтиды. "Revoked" мәртебесінің болуы теріс тексеру нәтижесін білдіреді. " Unknown" мәртебесі OCSP сервисінде тексерілетін сертификаттың мәртебесі туралы мәліметтердің жоқтығын білдіреді; "unknown" мәртебесі сертификатты қайтарып алу туралы мәліметтердің жоқтығын растауға мүмкіндік бермейтіндіктен, оның болуы тексерудің теріс нәтижесін де білдіреді.

Осы тармақта көзделген барлық тексерулердің оң нәтижесі болған кезде OCSP-түбіртекті тексеру нәтижесі оң болып табылады. Теріс нәтиже болса, көрсетілген тексерулердің кем дегенде біреуі OCSP түбіртегін тексеру нәтижесі теріс болып табылады.

20. ЭЦҚ-ның түпнұсқалығын тексерудің оң нәтижесі және Кодекстің 49-бабының 2-тармағында көзделген шарттар сақталған кезде электрондық құжатқа өзі қол қойылған құжатқа тең деп танылады және бірдей заңды күшке ие болады.

21. Кодекстің 61-бабының 2-тармағына сәйкес заңды тұлғаның атынан электрондық құжатқа қол қойған тұлғаның өкілеттіктерін тексерудің теріс нәтижесі ЭЦҚ

түпнұсқалығын тексеру нәтижесіне әсер етпейді. Тиісті өкілеттіктердің болмауының құқықтық салдары Қазақстан Республикасының заңнамасына сәйкес айқындалады.

22. Цифрлық жүйені пайдалана отырып, ЭЦҚ-ны қалыптастыру және (немесе) оның түпнұсқалығын тексеру кезінде цифрлық жүйенің иегері ЭЦҚ-ны қалыптастыру және (немесе) оның түпнұсқалығын тексеру процестеріне осы Қағидалардың талаптарының сақталуын қамтамасыз етеді.

23. ЭЦҚ сертификатының иегері цифрлық жүйені пайдаланбай дербес қалыптастырған жағдайда, ЭЦҚ қалыптастыру кезінде осы Қағидалардың талаптарының сақталуын сертификат иегерімен қамтамасыз етіледі. ЭЦҚ-ның түпнұсқалығын цифрлық жүйені пайдаланбай тексерген жағдайда, осы Қағидалардың талаптарының сақталуын осындай тексеруді жүзеге асыратын тұлғамен қамтамасыз етіледі.

24. ЭЦҚ туралы мәліметтердің бейнелі нысанда ұсынылуы, штрих-кодты, екі өлшемді матрицалық штрих-кодты немесе графикалық кескінді қоса алғанда, осы Қағидаларға сәйкес ЭЦҚ-ның түпнұсқалығын тексерудің дербес құралы ретінде пайдаланылмайды.

Егер цифрлық жүйе электрондық құжатқа қол қою кезінде штрих-кодты, екі өлшемді матрицалық штрих кодты немесе оны алу үшін қажетті электрондық құжатты не мәліметтерді қамтитын графикалық бейнені қалыптастырған жағдайда, мұндай цифрлық жүйе Кодекстің 61-бабының 4-тармағына және осы Қағидаларға сәйкес оған қатысты ЭЦҚ түпнұсқалығын тексеру жүзеге асырылатын электрондық құжатты алу мүмкіндігін қамтамасыз етеді.