Еуразиялық экономикалық одақтың интеграцияланған ақпараттық жүйесінің сенім білдірілген үшінші тарапы қызметінің куәландырушы орталығы туралы

Еуразиялық экономикалық комиссия Алқасының 2018 жылғы 25 қыркүйектегі № 154 шешімі

Еуразиялық экономикалық одақ шеңберіндегі ақпараттық-коммуникациялық технологиялар және ақпараттық өзара іс-қимыл туралы хаттаманың (2014 жылғы 29 мамырдағы Еуразиялық экономикалық одақ туралы шартқа № 3 қосымша) 18-тармағын іске асыру мақсатында Еуразиялық экономикалық комиссия Алқасы **шешті:**

1. Қоса беріліп отырған Еуразиялық экономикалық одақтың интеграцияланған ақпараттық жүйесінің сенім білдірілген үшінші тарапы қызметінің куәландырушы орталығы туралы ереже бекітілсін.

2. Осы Шешім ресми жарияланған күнінен бастап күнтізбелік 30 күн өткен соң күшіне енеді.

Еуразиялық экономикалық комиссия Алқасының Төрағасы *Т. Саркисян*

Еуразиялық экономикалық
комиссия Алқасының
2018 жылғы 25 қыркүйектегі
№ 154 шешімімен
БЕКІТІЛГЕН

Еуразиялық экономикалық одақтың интеграцияланған ақпараттық жүйесінің сенім білдірілген үшінші тарапы қызметінің куәландырушы орталығы туралы ЕРЕЖЕ

I. Жалпы ережелер

1. Осы Ереже Еуразиялық экономикалық комиссияда (бұдан әрі – Комиссия) құрылатын Еуразиялық экономикалық одақтың интеграцияланған ақпараттық жүйесінің сенім білдірілген үшінші тарапы қызметінің (бұдан әрі тиісінше – Одақ, СҮТ қызметі) куәландырушы орталығының мақсаты мен негізгі міндеттерін, сондай-ақ оның құқықтарын, міндеттемелерін, жауапкершілігін және қызметін тоқтату тәртібін айқындайды.

2. СҮТ қызметі куәландырушы орталығының негізгі мақсаты Одақ шеңберінде электрондық құжаттармен халықаралық (трансшекаралық) алмасу кезінде электрондық цифрлық қолтаңбаны қолдана отырып, электрондық құжаттардың заңдық күшін қамтамасыз ету үшін Комиссияның сенім білдірілген үшінші тараптары мен СҮТ қызметі құрамындағы Одаққа мүше мемлекеттердің (бұдан әрі – мүше мемлекеттер) электрондық өзара іс-қимылын ұйымдастыру мақсатында Комиссияның сенім

білдірілген уәкілетті үшінші тараптарын және мүше мемлекеттерді электрондық цифрлық қолтаңбаны тексеру кілттерінің сертификаттарымен қамтамасыз ету болып табылады.

3. Осы Регламенттің мақсаттары үшін төмендегілерді білдіретін мынадай ұғымдар пайдаланылады:

"криптографиялық стандарт" – криптографиялық кілтті пайдалана отырып ақпаратты өзгерту, соның ішінде ЭЦҚ қалыптастыру және тексеру (криптографиялық өзгерту) қағидалары мен алгоритмдерін белгілейтін техникалық ерекшеліктердің жиынтығы;

"ЭЦҚ-ны тексеру кілтінің сертификаты" – куәландырушы орталық шығаратын, ЭЦҚ кілті пайдаланыла отырып куәландырушы орталықтың ЭЦҚ-мен қол қойылған және сертификатта көрсетілген ЭЦҚ-ны тексеру кілтінің белгілі бір электрондық іс-қимыл субъектісіне тиесілілігін растайтын ақпаратты және Комиссия Кеңесі бекітетін трансшекаралық сенім кеңістігін құрудың, дамытудың және оның жұмыс істеуінің тиісті криптографиялық стандарттары мен талаптарын көздейтін өзге де ақпаратты қамтитын электрондық құжат;

"куәландырушы орталық" – Комиссия актілеріне, мүше мемлекеттің заңнамасына сәйкес ЭЦҚ-ны тексеру кілттерінің сертификаттарын шығару, тарату, сақтау және осы сертификаттардың жарамдылығын тексеру бойынша қызметтер көрсетуді қамтамасыз ететін уәкілетті орган немесе ұйым;

"электрондық цифрлық қолтаңба (электрондық қолтаңба)", "ЭЦҚ" – электрондық түрдегі басқа ақпаратқа қосылған немесе осындай ақпаратпен өзге де түрде байланысқан, осы ақпараттың тұтастығын және түпнұсқалылығын бақылау үшін қызмет ететін, авторлықтан бас тартудың мүмкін еместігін қамтамасыз ететін, жабық (жеке) кілт пайдаланыла отырып осы ақпаратқа қатысты криптографиялық өзгертуді қолдану жолымен дайындалатын және ашық кілт (ЭЦҚ-ны тексеру кілті) пайдаланыла отырып тексерілетін электрондық түрдегі ақпарат.

Осы Ережеде пайдаланылатын өзге де ұғымдар Еуразиялық экономикалық одақ шеңберіндегі ақпараттық-коммуникациялық технологиялар және ақпараттық өзара іс-қимыл туралы хаттамада (2014 жылғы 29 мамырдағы Еуразиялық экономикалық одақ туралы шартқа № 3 қосымша), Еуразиялық экономикалық комиссия Кеңесінің 2014 жылғы 18 қыркүйектегі № 73 шешімімен бекітілген Мемлекетаралық ақпараттық өзара іс-қимыл кезінде сервистерді және заңды күші бар электрондық құжаттарды пайдалану тұжырымдамасында және трансшекаралық сенім кеңістігін құруға, дамытуға және оның жұмыс істеуіне қойылатын талаптарда айқындалған мәндерде қолданылады.

4. Электрондық құжаттарды ресімдеу трансшекаралық сенім кеңістігін құруға, дамытуға және оның жұмыс істеуіне қойылатын талаптарға және Еуразиялық экономикалық комиссия Алқасының 2015 жылғы 28 қыркүйектегі № 125 шешімімен бекітілген Еуразиялық экономикалық одаққа мүше мемлекеттердің мемлекеттік билік

органдарының бір-бірімен және Еуразиялық экономикалық комиссиямен трансшекаралық өзара іс-қимылы кезінде электрондық құжаттармен алмасу туралы ережеге сәйкес жүзеге асырылады.

5. СҮТ қызметі куәландырушы орталығының функцияларын Комиссияның Ақпараттық технологиялар департаменті жүзеге асырады.

II. СҮТ қызметі куәландырушы орталығының негізгі міндеттері

6. Мыналар:

а) ЭЦҚ-ны тексерудің ашық кілтінің жабық (жеке) кілтке сәйкестігін куәландыру, сондай-ақ Комиссияның сенім білдірілген үшінші тарапы мен мүше мемлекеттердің сенім білдірілген үшінші тараптарының ЭЦҚ-ны тексеру кілттері сертификаттарының түпнұсқалылығын растау;

б) СҮТ қызметі шеңберінде электрондық құжаттармен халықаралық (трансшекаралық) алмасу кезінде Комиссияның сенім білдірілген үшінші тарапы мен мүше мемлекеттердің сенім білдірілген үшінші тараптарының ЭЦҚ-ны тексеру кілттерінің сертификаттарына сенім кепілдіктерін қамтамасыз ету;

в) Комиссияның сенім білдірілген үшінші тарапы мен мүше мемлекеттердің сенім білдірілген үшінші тараптарының сұрау салулары бойынша ЭЦҚ-ны тексеру кілттерінің сертификаттарын шығару, тарату және сақтау, сондай-ақ осы сертификаттардың жарамдылығын тексеру;

г) Комиссияның сенім білдірілген үшінші тарапы мен мүше мемлекеттердің сенім білдірілген үшінші тараптарының сұрау салулары бойынша ЭЦҚ-ны тексеру кілттерінің сертификаттарында көрсетілген мәліметтердің дұрыстығын растау СҮТ қызметі куәландырушы орталығының негізгі міндеттері болып табылады.

III. СҮТ қызметі куәландырушы орталығының құқықтары, міндеттері және жауапкершілігі

8. Өз функцияларын жүзеге асыру мақсатында СҮТ қызметі куәландырушы орталығының:

а) пайдаланушылар (Комиссияның және мүше мемлекеттердің сенім білдірілген үшінші тараптарының өкілдері) ЭЦҚ-ны тексеру кілттерінің сертификаттарын алу мақсатында ұсынатын мәліметтерді тексеруді жүргізуге;

б) пайдаланушылар ЭЦҚ-ны тексеру кілттерінің сертификаттарын алу үшін сенімсіз мәліметтер немесе толық емес көлемде мәліметтер берген жағдайда, оларға ЭЦҚ-ны тексеру кілттерінің сертификаттарын беруден бас тартуға;

в) мынадай:

ЭЦҚ-ны тексеру кілтінің құпиялылығының бұзылғаны туралы сенімді мәліметтер және (немесе) ЭЦҚ-ны тексеру кілттерінің сертификаттарын одан әрі пайдалану мүмкіндігіне елеулі түрде әсер етуі мүмкін өзге де мәліметтер алынған;

ЭЦҚ-ны тексеру кілттері заңды күшінен айрылған;

ЭЦҚ-ның тиісті құралдары жоғалған;

сертификаттың иесі туралы мәліметтер өзгерген;

Регламентте немесе Одақ органдарының актілерінде белгіленген өзге де жағдайларда ЭЦҚ-ны тексеру кілттерінің берілген сертификаттарының қолданысын тоқтатуға немесе күшін жоюға;

г) СҮТ қызметі куәландырушы орталығының құралдарын пайдалану кезінде пайдаланушылардың ақпараттық қауіпсіздікке қойылатын талаптарды сақтауын қамтамасыз етуге және бақылауға;

д) СҮТ қызметі куәландырушы орталығы жұмысының мәселелерін регламенттейтін құжаттарды әзірлеуге және келісуге қатысуға;

е) СҮТ қызметі куәландырушы орталығының ЭЦҚ-ны тексеру кілтінің түбір сертификатының және пайдаланушылардың ЭЦҚ-ны тексеру кілттері сертификаттарының қолданылу мерзімін белгілеуге құқығы бар.

9. СҮТ қызметінің куәландырушы орталығы өз функцияларын жүзеге асыру кезінде :

а) пайдаланушылар ұсынған құжаттардың (оларда көрсетілген мәліметтерді міндетті түрде тексерумен) негізінде оларды белгіленген тәртіппен СҮТ қызметінің куәландырушы орталығына тіркеуді қамтамасыз етуге;

б) ЭЦҚ-ны және ЭЦҚ құралдарын пайдалану тәртібі туралы, ЭЦҚ-ны пайдаланумен байланысты тәуекелдер және ЭЦҚ қауіпсіздігін қамтамасыз ету және оны тексеру үшін қажетті шаралар туралы Комиссияның және мүше мемлекеттердің сенім білдірілген үшінші тараптарын жазбаша нысанда хабардар етуге;

в) Комиссияның және мүше мемлекеттердің сенім білдірілген үшінші тараптарын СҮТ қызметі куәландырушы орталығының жұмыс тәртібімен таныстыруға;

г) Комиссияның және мүше мемлекеттердің сенім білдірілген үшінші тараптарын ЭЦҚ-ны тексеру кілттері сертификаттарының тізілімінде қамтылған ақпаратты өзекті етуге және оны заңсыз енуден, жоюдан өзгертуден, бұғаттаудан және өзге де заңсыз әрекеттерден қорғауды қамтамасыз етуге;

д) Комиссияның сенім білдірілген үшінші тарапының және мүше мемлекеттердің сенім білдірілген үшінші тараптарының ЭЦҚ-ны тексеру кілттері сертификаттарының тізіліміндегі ақпаратты, соның ішінде ЭЦҚ-ны тексеру кілттері сертификаттарының күшін жою туралы ақпаратты кез келген адамға оның өтініші бойынша ұсынуға;

е) СҮТ қызметінің куәландырушы орталығы жасаған ЭЦҚ-ны тексеру кілттері сертификаттарының құпиялылығын қамтамасыз етуге;

ж) ЭЦҚ-ны тексеру кілттерінің сертификаттарын шығару, олардың мәртебесін тексеру, қолданысын тоқтату, қалпына келтіру және күшін жою техникалық рәсімдерін толық көлемде орындауды, сондай-ақ ЭЦҚ-ны тексеру кілттері сертификаттарының күшін жою туралы ақпаратты жариялауды қамтамасыз етуге;

з) пайдаланушылардың сұрау салулары бойынша Комиссияның сенім білдірілген үшінші тарапының және мүше мемлекеттердің сенім білдірілген үшінші тараптарының ЭЦҚ-ны тексеру кілттерінің сертификаттарын қолданумен байланысты даулы жағдайларды шешуге қатысуға;

и) Комиссияның куәландырушы орталығы жасаған ЭЦҚ-ны тексеру кілттерінің сертификаттарын, ЭЦҚ-ны тексеру кілттерінің сертификаттары олардың негізінде шығарылған қағаз жеткізгіштегі құжаттарды және СҮТ қызметінің куәландырушы орталығының өзге де құжаттарын 15 жыл бойына сақтауды қамтамасыз етуге (Комиссия белгілеген мұрағаттық сақтау мерзімі өткен құжаттарды жою тәртібін сақтай отырып);

к) пайдаланушының жеке басын куәландыратын негізгі құжаттың деректемелерін кемінде 15 жыл бойы сақтауға;

л) осы сертификатқа сәйкес келетін ЭЦҚ кілтінің құпиясы ашылған жағдайда, СҮТ қызметі куәландырушы орталығының ЭЦҚ-ны тексеру кілті сертификатының күшін жоюға міндетті.

10. СҮТ қызметінің куәландырушы орталығы:

а) осы Ережеде және Одақ органдарының ЭЦҚ-ны қолдануды реттеу саласындағы актілерінде көзделген міндеттемелердің орындалмауы немесе тиісті дәрежеде орындалмауы;

б) ЭЦҚ құралдарын және СҮТ қызметі куәландырушы орталығының құралдарын пайдалану кезінде ақпараттың қауіпсіздігі жұмыстарын және оны бақылауды тиісті түрде ұйымдастырмау;

в) СҮТ қызметі куәландырушы орталығының аппараттық және бағдарламалық-техникалық құралдарын пайдалану қағидаларын СҮТ қызметі куәландырушы орталығының сақтамауы нәтижесінде үшінші тұлғаларға зиян келтірілген жағдайда Одақ органдарының актілеріне сәйкес жауапкершілік көтереді.

IV. СҮТ қызметі куәландырушы орталығының өзге тұлғалармен өзара іс-қимылы

11. СҮТ қызметінің куәландырушы орталығы Комиссияның құрылымдық бөлімшелерімен СҮТ қызметі куәландырушы орталығының құзыретіне жатқызылған мәселелер бойынша өзара іс-қимыл жасайды.

12. СҮТ қызметінің куәландырушы орталығы өз функцияларын жүзеге асыру мақсатында Регламентке сәйкес өз атынан ашық кілттер инфрақұрылымына өзге де қатысушылармен (мүше мемлекеттердің сенім білдірілген үшінші тараптарымен) өзара іс-қимыл жасайды.

V. СҮТ қызметі куәландырушы орталығының жұмысын тоқтату

13. СҮТ қызметі куәландырушы орталығының жұмысы Комиссия Алқасының шешімі бойынша тоқтатылады.

14. СҮТ қызметінің куәландырушы орталығы жұмысының тоқтатылғаны туралы шешім қабылданған жағдайда жұмысы тоқтатылған күнге дейін 1 айдан кешіктірмей Комиссияның сенім білдірілген үшінші тарапын және мүше мемлекеттердің сенім білдірілген үшінші тараптарын ол туралы хабардар етеді.

15. СҮТ қызметі куәландырушы орталығының функциялары басқа куәландырушы орталыққа берілген жағдайда Комиссияның сенім білдірілген үшінші тарапының және мүше мемлекеттердің сенім білдірілген үшінші тараптарының СҮТ қызметінің куәландырушы орталығының жұмысын тоқтату күнінде шығарылған ЭЦҚ-ны тексеру кілттері сертификаттарының тізілімі де беріледі.

16. СҮТ қызметі куәландырушы орталығының ақпараттық жүйелері таратылған жағдайда Комиссияның сенім білдірілген үшінші тарапының және мүше мемлекеттердің сенім білдірілген үшінші тараптарының ЭЦҚ-ны тексеру кілттері сертификаттарының тізілімі, сондай-ақ СҮТ қызметі куәландырушы орталығының басқа да электрондық құжаттары мен қағаз жеткізгіштегі құжаттары Комиссияда белгіленген тәртіппен мұрағаттық сақтауға беріледі.

Еуразиялық экономикалық
одақтың интеграцияланған
ақпараттық жүйесінің сенім
білдірілген үшінші тарапы
қызметінің куәландырушы
орталығы туралы ережеге
ҚОСЫМША

Еуразиялық экономикалық одақтың интеграцияланған ақпараттық жүйесінің сенім білдірілген үшінші тарапы қызметі куәландырушы орталығының РЕГЛАМЕНТІ

I. Жалпы ережелер

1. Осы Регламент Еуразиялық экономикалық одақтың интеграцияланған ақпараттық жүйесінің сенім білдірілген үшінші тарапы (СҮТ) қызметінің куәландырушы орталығы (бұдан әрі тиісінше – ақпараттық жүйе, СҮТ қызметінің КО-сы) берген сертификаттар пайдаланылатын ашық кілттер инфрақұрылымына қатысушылардың өзара іс-қимыл жасау тәртібін, электрондық цифрлық қолтаңбаны (электрондық қолтаңба) (бұдан әрі – ЭЦҚ) тексеру кілттерінің сертификаттарын шығару, көрсетілген сертификаттарды сүйемелдеу кезінде СҮТ қызметінің КО-сы пайдаланатын негізгі рәсімдер мен ұйымдастыру-техникалық іс-шаралардың деректер форматтары мен жұмыс хаттамаларының сипаттамасын белгілейді.

Осы Регламент RFC 3647. "Certificate Policy and Certification Practices Framework" ұсынымдарына (Сертификаттар беру саясаты және сертификациялық практикалар жөніндегі ұсынымдар) сәйкес дайындалды.

1.1. Құжаттың атауы және сәйкестендіру

Құжаттың атауы: Еуразиялық экономикалық одақтың интеграцияланған ақпараттық жүйесінің сенім білдірілген үшінші тарапы қызметінің куәландырушы орталығының регламенті.

Қысқартылған атауы: СҮТ қызметі КО-сының регламенті.

1.2. Интеграцияланған жүйенің ашық кілттері инфрақұрылымына қатысушылар

МСЭ-Т Х.509 "Ақпараттық технологиялар – Ашық жүйелердің өзара байланысы – Анықтамалық: Ашық кілттер мен атрибуттар сертификаттарының құрылымы" ұсынымына сәйкес интеграциялық жүйе ашық кілттерінің инфрақұрылымы (бұдан әрі – АКИ) деп Одақтың бірыңғай сенім кеңістігі шеңберінде авторлықты түпнұсқаландыру, шифрлау қызметтерін, оның тұтастығын немесе тіркелуін қолдау үшін ашық кілттерді басқаруды ұстап тұруға қабілетті инфрақұрылым түсініледі.

1.2.1. Куәландырушы орталық

СҮТ қызметінің КО-сы – СҮТ уәкілеттік берген Комиссияның интеграциялық сегменті мен Одаққа мүше мемлекеттердің (бұдан әрі – мүше мемлекеттер) ұлттық сегменттерінің өзара іс-қимылы үшін ЭЦҚ-ны тексеру кілттерінің сертификаттарымен қамтамасыз ету жөніндегі функцияларды жүзеге асыратын Еуразиялық экономикалық комиссияның (бұдан әрі – Комиссия) Ақпараттық технологиялар департаментінің құрамындағы бөлім.

СҮТ қызметі КО-сының негізгі функцияларына:

Комиссияның сенім білдірілген үшінші тарапын және мүше мемлекеттердің сенім білдірілген үшінші тараптарын тіркеу;

Комиссияның сенім білдірілген үшінші тарапының және мүше мемлекеттердің сенім білдірілген үшінші тараптарының сұрау салулары бойынша ЭЦҚ-ны тексеру кілттерінің сертификаттарын жасау және беру;

Комиссияның сенім білдірілген үшінші тарапының және мүше мемлекеттердің сенім білдірілген үшінші тараптарының атынан ЭЦҚ-ны тексеру кілтінің сертификатын алу үшін өтініш жасайтын адамдардың өкілеттіктерін айқындау және Комиссия бекітетін, сенім білдірілген үшінші тарап куәландырушы орталығының жұмыс істеуін регламенттейтін құжаттарға сәйкес көрсетілген өкілеттіктер туралы ақпаратты сақтау;

ЭЦҚ-ны тексеру кілтінің сертификатын жасауға және алуға берілген сұрау салуда тиісті сенім білдірілген үшінші тарап көрсеткен ЭЦҚ-ны тексеру кілтіне сәйкес келетін ЭЦҚ кілтінің иелілігін растау және осы кілттің иелілігін растау кезінде теріс нәтиже болған жағдайда көрсетілген сертификатты жасаудан бас тарту;

ЭЦҚ-ны тексеру кілттері сертификаттарының қолданылу мерзімдерін белгілеу. ЭЦҚ-ны тексеру кілтінің сертификаты, егер сертификаттың өзінде осындай сертификаттың қолданысы басталуының өзге күні көрсетілмесе, ол берілген сәттен бастап қолданылады, бұл ретте ЭЦҚ-ны тексеру кілтінің сертификаты туралы ақпаратты сенім білдірілген үшінші тарап қызметінің куәландырушы орталығы онда

көрсетілген осындай сертификат қолданысының басталатын күнінен кешіктірмей ЭЦҚ-ны тексеру кілттерінің берілген, қолданысын тоқтатқан және күші жойылған сертификаттарының тізіліміне (бұдан әрі – сертификаттар тізілімі) енгізуге тиіс;

ЭЦҚ-ны тексеру кілттері сертификаттарының қолданылуын тоқтату және күшін жою;

сертификаттар тізілімін оған сенім білдірілген үшінші тарап қызметінің куәландырушы орталығы берген ЭЦҚ-ны тексеру кілттерінің сертификаттарында қамтылған ақпаратты, сондай-ақ осындай сертификаттардың қолданысын тоқтату немесе күшін жою туралы және қолданысын тоқтату немесе күшін жою негіздемелері туралы ақпаратты енгізе отырып жүргізу;

ЭЦҚ-ны тексеру кілттерінің қолданысын тоқтатқан және күші жойылған сертификаттарының тізімін (бұдан әрі – кері қайтарылған сертификаттардың тізімі) жүргізу;

сертификаттар тізіліміне және кері қайтарылған сертификаттар тізіміне тиісті өзгерістер енгізілгенге дейін ЭЦҚ-ны тексеру кілті сертификатының иесіне оның сертификатының күші жойылғаны туралы хабарлау;

сертификаттар тізіліміндегі ЭЦҚ-ны тексеру кілттерінің бірегейлігін тексеру және Комиссияның сенім білдірілген үшінші тарапының және мүше мемлекеттердің сенім білдірілген үшінші тараптарының сұрау салуында көрсетілген ЭЦҚ-ны тексеру кілтінің бірегейлігін тексерудің теріс нәтижесі жағдайында ЭЦҚ-ны тексеру кілтінің сертификатын жасаудан бас тарту;

сертификаттар тізіліміндегі және кері қайтарылған сертификаттар тізіміндегі ақпаратты өзекті ету, сондай-ақ оны заңсыз енуден, жоюдан, өзгертуден, бұғаттаудан және өзге де заңсыз әрекеттерден қорғау;

сенім білдірілген үшінші тарап қызметінің куәландырушы орталығы қызметінің бүкіл мерзімі ішінде сертификаттар тізіліміне енгізілген ақпаратты сақтау;

Комиссияның сенім білдірілген үшінші тарапының және мүше мемлекеттердің сенім білдірілген үшінші тараптарының кез келген уақытта интеграцияланған жүйе құралдарын пайдалана отырып сертификаттар тізіліміне тегін негізде қол жеткізуі;

Комиссияның сенім білдірілген үшінші тарапының және мүше мемлекеттердің сенім білдірілген үшінші тараптарының өтініштері бойынша ЭЦҚ-ны тексеруді жүзеге асыру;

Комиссияның сенім білдірілген үшінші тарапы және мүше мемлекеттердің сенім білдірілген үшінші тараптары электрондық құжаттар дайындау және оларға тиісті ЭЦҚ қол қою уақытын растау мақсатында өтініш жасаған жағдайда осындай сенім білдірілген үшінші тараптардың түбіртектеріне уақыт штамптарын жасау;

ЭЦҚ-ны тексеру кілттерінің берілген сертификаттарын басқарумен байланысты өзге де қызметті жүзеге асыру жатады.

1.2.2. Ашық кілттер инфрақұрылымын пайдаланушылар

Ашық кілттер инфрақұрылымын (АКИ) пайдаланушылар: сертификаттардың иелері және сенім білдіруші тараптар деген екі санатқа бөлінеді.

СҮТ қызметінің КО-сы беретін ЭЦҚ-ны тексеру кілттері сертификаттарының иелері мынадай субъектілер (кілт жұптарын генерациялауды, сертификат алуға сұрау салу қалыптастыруды, өзінің жұмыс орнында СҮТ қызметі КО-сының сертификатын орнатуды және ЭЦҚ-ны тексеру кілттерінің сертификаттары иелерінің құқықтары мен міндеттеріне сәйкес басқа да операцияларды жүзеге асыратын) болып табылады:

Комиссияның сенім білдірілген үшінші тарапы;

мүше мемлекеттердің сенім білдірілген үшінші тараптары (уәкілетті ұйымдар – тиісті сервистердің операторлары);

СҮТ қызметінің КО-сы.

Криптографиялық кілттерді қалыптастырумен, электрондық-цифрлық қолтаңбаларды (электрондық қолтаңбаларды) тексеру кілттерінің сертификаттарын дайындауға сұрау салулар қалыптастырумен, электрондық-цифрлық қолтаңбаларды (электрондық қолтаңбаларды) тексеру кілттерінің сертификаттарын алумен, электрондық-цифрлық қолтаңбаларды (электрондық қолтаңбаларды) тексеру кілттері сертификаттарының көрсетілген иелері атынан электрондық-цифрлық қолтаңбаларды (электрондық қолтаңбаларды) тексеру кілттері сертификаттарының қолданысын тоқтатуға және күшін жоюға сұрау салуларды алумен байланысты операцияларды осы Регламенттің 23.2-тармағында сипатталған тәртіппен өкілеттіктері расталатын уәкілетті тұлғалар орындайды.

ЭЦҚ-ны тексеру кілттері сертификаттарының иелері АКИ басқа пайдаланушыларының ЭЦҚ-сын тексеру рәсімдерін жүргізу кезінде СҮТ қызметінің КО-сынан сертификаттар мен ашық кілттердің мәртебесі туралы ақпаратты (ЭЦҚ тексеру және электрондық құжаттың түпнұсқалылығы туралы шешім қабылдау кезінде соған сене отырып) сұрататын сенім білдіруші тараптар болып табылады.

Интеграцияланған жүйе интеграциялық сегментінің АКИ-інде басқа сенім білдіруші тараптар жоқ.

1.2.2.1. Комиссияның сенім білдірілген үшінші тарапы және мүше мемлекеттердің сенім білдірілген үшінші тараптары

Комиссияның интеграциялық сегментінің және мүше мемлекеттердің ұлттық сегменттерінің құрамында жұмыс істейтін, субъектілердің Одақтың интеграцияланған ақпараттық жүйесі құралдарымен өзара іс-қимылының электрондық нысаны кезінде ЭЦҚ бірыңғай трансшекаралық сенім кеңістігін қамтамасыз ететін СҮТ сервистерінің жиынтығы интеграцияланған ақпараттық жүйенің СҮТ бірыңғай қызметін (бұдан әрі – СҮТ қызметі) білдіреді.

СҮТ қызметі шеңберінде мүше мемлекеттердің СҮТ-і атынан мүше мемлекеттер және Комиссияның СҮТ-і атынан Комиссия СҮТ сервистерін ұсынады.

Мүше мемлекеттер СҮТ сервистерінің операторлары уәкілетті органдар немесе олар айқындаған (аккредиттеген) ұйымдар болып табылады.

Комиссия СҮТ сервистерінің операторлары Комиссия болып табылады.

Интеграцияланған жүйе шеңберінде СҮТ қызметінің негізгі міндеттері:

ақпараттық өзара іс-қимыл субъектілерінің – интеграцияланған жүйенің шеңберінде тіркелген уақыт сәтінде куәландырушы орталықтар шығарған сертификаттар иелерінің электрондық құжаттарының және ЭЦҚ түпнұсқалылығын және өзектілігін растау;

электрондық құжаттармен халықаралық (трансшекаралық) алмасуда сенім кепілдіктерін қамтамасыз ету;

мүше мемлекеттердің заңнамасына және Комиссия актілеріне сәйкес шығыс және (немесе) кіріс электрондық құжаттарда ЭЦҚ қолданудың заңдылығын қамтамасыз ету болып табылады.

СҮТ сервисі серверінің сертификаты (СҮТС серверінің сертификаты) түбіртектер мен сұрау салулардың құрамына кіреді және осы түбіртектер мен сұрау салулардағы ЭЦҚ-ны тексеру, сондай-ақ СҮТ сервисінің серверін сәйкестендіру үшін пайдаланылады.

1.2.2.2. Уақыт штамптары сервисі

Интеграцияланған жүйенің ашық кілттері инфрақұрылымында уақыт штамптары сервистері іске асырылған. Уақыт штамптары сервистері RFC 3161 (Time-Stamp Protocol) ұсынымдарына – уақыт штамптары хаттамасына сәйкес уақыт штамптарын тудырады. Әрбір уақыт штампы уақыт штамптарының сервистері үшін арнайы жасалған ЭЦҚ кілттерінің көмегімен ғана куәландырылады.

1.2.2.3. Сертификат мәртебесін тексеру сервисі

Интеграцияланған жүйенің ашық кілттері инфрақұрылымында сертификаттың мәртебесін кері қайтарылған сертификаттардың тізімі бойынша тексеру әдісінен басқа, сертификаттың мәртебесін онлайн-режимде (OCSP) тексеру бойынша сервис ұсынылады. Сертификаттың мәртебесін тексеру сервисінің барлық жауаптарына сертификаттың мәртебесін тексеру сервисі үшін арнайы жасалған ЭЦҚ кілттерінің көмегімен қол қойылады.

1.2.3. Сертификаттарды пайдалану

СҮТ қызметінің КО шығаратын сертификаттарды СҮТ операторлары СҮТ қызметінің жұмыс істеуін қамтамасыз ету мақсатында СҮТ операторлары пайдаланады

.

Сертификаттарды пайдалану салалары СҮТ қызметі КО-сының басшылары бекітетін, сертификаттар соларға сәйкес берілетін саясаттарға тәуелді болады.

СҮТ қызметінің КО-сы сертификаттарды ЭЦҚ-ны тексеру кілттері сертификаттарының мынадай саясаттарына сәйкес береді:

СҮТ қызметі КО-сының сертификаттау сервисінің ЭЦҚ-ны тексеру кілттерінің сертификаттары (бұдан әрі – КО уәкілетті тұлғаларының сертификаттары, КО түбір сертификаттары);

СҮТ сервисі (СҮТС) серверінің ЭЦҚ-ны тексеру кілттерінің сертификаттары;

сертификаттың мәртебесін тексеру сервисінің (СМТС) ЭЦҚ-ны тексеру кілттерінің сертификаттары;

уақыт штамптары сервисінің (УШС) ЭЦҚ-ны тексеру кілттерінің сертификаттары.

СҮТ қызметі КО-сының сертификаттау сервисінің ЭЦҚ-ны тексеру кілттерінің сертификаттары сертификаттардағы және кері қайтарылған сертификаттар тізімдеріндегі (бұдан әрі – КСТ) электрондық-цифрлық қолтаңбаларды тексеруге арналған.

СҮТС серверінің ЭЦҚ-ны тексеру кілттерінің сертификаттары түбіртектердегі ЭЦҚ-ны тексеруге және СҮТ сервисінің серверін сәйкестендіруге арналған. СҮТС серверінің ЭЦҚ-ны тексеру кілттерінің сертификаттары сондай-ақ СҮТ операторларынан СҮТ қызметінің КО-сына келіп түсетін сертификаттарды шығаруға және кері қайтаруға сұрау салудың қолтаңбаларын тексеру үшін де пайдаланылады.

СМТС ЭЦҚ-ны тексеру кілттерінің сертификаттары сертификаттардың мәртебесін тексеру сервисі беретін жауаптардағы электрондық цифрлық қолтаңбаларды тексеруге арналған.

УШС ЭЦҚ-ны тексеру кілттерінің сертификаттары интеграцияланған жүйенің интеграциялық және ұлттық сегменттерінің уақыт штамптары сервисі беретін уақыт штамптарындағы электрондық цифрлық қолтаңбаларды тексеруге арналған.

СҮТ қызметінің КО-сы берген, СҮТ қызметі КО-сының басшылары бекітетін саясаттарда көзделмеген, №1 қосымшаға сәйкес көзделген сертификат соларға сәйкес шығарылған сертификаттарды пайдалануға жол берілмейді.

1.3. Құжатты басқару

СҮТ қызметі КО-сының Регламентін басқаратын ұйым: Еуразиялық экономикалық комиссияның Ақпараттық технологиялар департаменті.

СҮТ қызметі куәландырушы орталығының мекенжайы:

115114, Мәскеу қаласы, Летниковская көшесі, 2-үй, 1-құр., 2-құр.

Телефон: +7 (495) 669-24-00, доб. _____

Факс: 8 (495) 669-24-15

e-mail: info@eecommission.org

СҮТ қызметі куәландырушы орталығының пошта және заңды

мекенжайы: 119121, Мәскеу қаласы, Смоленск бульвары, 3/5-үй, 1-құр.

Байланысушы адам: _____

СҮТ қызметі КО-сының Регламентін бекіту рәсімі:

СҮТ қызметі КО-сының осы Регламентін және сертификаттар саясаттарын бекітуді, сондай-ақ оларға өзгерістер енгізуді белгіленген тәртіппен Комиссия жүзеге асырады. Өзгерістер репозиторийде құжаттың жаңа нұсқасы түрінде жарияланады.

1.4. Белгіленімдер, терминдер және айқындамалар

Осы Регламентте Еуразиялық экономикалық одақ шеңберіндегі ақпараттық-коммуникациялық технологиялар және ақпараттық өзара іс-қимыл туралы хаттамада (2014 жылғы 29 мамырдағы Еуразиялық экономикалық одақ туралы шартқа № 3 қосымша) келтірілген ұғымдар және мынадай терминдер мен айқындамалар пайдаланылады:

"сенім білдіруші тарап" – ЭЦҚ тексеретін ашық кілттер инфрақұрылымын пайдаланатын ақпараттық өзара іс-қимылға қатысушы;

"электрондық цифрлық қолтаңбаны тексеру кілті сертификатының иесі" – ЭЦҚ-ны тексеру кілтінің сертификаты берілген тұлға;

"өтініш беруші" – СҮТ қызметінің КО-сына сертификат шығаруға өтініш беретін жеке тұлға;

"электрондық цифрлық қолтаңбаны тексеру кілті (ашық кілт, ЭЦҚ-ны тексеру кілті" – электрондық цифрлық қолтаңба кілтімен бір текті байланысты және электрондық цифрлық қолтаңбаның түпнұсқалылығын тексеруге арналған символдардың бірегей дәйектілігі;

"электрондық цифрлық қолтаңба кілті (ЭЦҚ кілті)" – символдардың ЭЦҚ жасауға арналған бірегей дәйектілігі;

"кілттер жұбы" – ЭЦҚ-ны тексеру кілті және ЭЦҚ кілті;

"ЭЦҚ кілтінің компрометациясы" – ЭЦҚ кілтінің құпиясы ашылуы мүмкін деуге негіз беретін факт;

"КО пайдаланушы" – сертификаттың иесі немесе өтініш беруші;

"электрондық цифрлық қолтаңбаны тексеру кілтінің сертификаты (сертификат)" – 3-нұсқаның X.509 стандартына сәйкес қалыптастырылған, ашық кілтті және оның иесінің сәйкестендіру деректерін қамтитын және КО уәкілетті тұлғасының ЭЦҚ-сымен қол қойылған электрондық құжат;

"кері қайтарылған сертификаттар тізімі, КСТ" – ЭЦҚ-ны тексеру кілттерінің қолданысын тоқтатқан және күші жойылған сертификаттарының тізімі;

"ЭЦҚ құралдары" – ең болмағанда мына функциялардың бірін: ЭЦҚ жасауды, ЭЦҚ-ны тексеруді, ЭЦҚ кілтін жасауды және ЭЦҚ-ны тексеру кілтін жасауды іске асыру үшін пайдаланылатын криптографиялық құралдар;

"уақыт штампы" – бұл деректердің белгілі бір уақытқа дейін өмір сүретіндігінің дәлелдемесі (RFC 3161 " Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" сәйкес);

"электрондық цифрлық қолтаңба (электрондық қолтаңба) (ЭЦҚ)" – басқа ақпаратқа (қол қойылатын ақпаратқа) электрондық нысанда қосылған немесе осындай ақпаратпен өзге де түрде байланысқан және қол қойған адамды айқындау үшін пайдаланылатын электрондық нысандағы ақпарат.

II. СҮТ қызметінің КО-сы көрсететін қызметтердің тізбесі

2. Осы Регламенттің 1.2.1-тармағында көзделген негізгі функциялардың тізбесіне сәйкес көрсетілетін СҮТ қызметі КО-сының қызметтерін қамтамасыз ету үшін СҮТ қызметінің КО-сында мынадай функционалдық құрамдастар (сервистер) іске асырылған:

сертификаттар сервисі;

уақыт штамптары сервисі;

сертификаттардың мәртебесін тексеру сервисі;

тіркеу сервисі;

сертификаттау сервисі;

ақпаратты қорғау жүйесі;

ЭЦҚ құралдары.

Сертификаттар сервисі мүше мемлекеттер ұлттық сегменттерінің СҮТ-і және Комиссияның СҮТ-і тарапынан ЭЦҚ-ны тексеру кілттері сертификаттарының тізіліміне және кері қайтарылған сертификаттардың тізіміне қол жеткізуді қамтамасыз етеді.

Уақыт штамптары сервисі мүше мемлекеттер ұлттық сегменттерінің СҮТ-і және Комиссияның СҮТ-і үшін ЭЦҚ қалыптастыру операцияларын орындау кезінде уақыт штамптарын алуға арналған интерфейс ұсынады.

Сертификаттардың мәртебесін тексеру сервисі мүше мемлекеттер ұлттық сегменттерінің СҮТ-і және Комиссияның СҮТ-і үшін OCSP хаттамасын пайдалана отырып күші жойылған сертификаттардың сұрау салуынсыз сертификаттың мәртебесін нақты уақыт режимінде тексеру мүмкіндігін береді.

Тіркеу сервисі сертификаттарды беруге және олардың мәртебесін өзгертуге сұрау салуларды тіркеу мүмкіндігін береді. Сервис мүше мемлекеттердің ұлттық сегменттері СҮТ-інің және Комиссия СҮТ-інің тіркеу деректерін, ЭЦҚ-ны тексеру кілттерінің сертификаттарын жасауға сұрау салуларды сақтауды қамтамасыз етеді.

Сертификаттау сервисі ЭЦҚ-ны тексеру кілттері сертификаттарының эталондық базасын және күші жойылған сертификаттардың тізімдерін сақтауды қамтамасыз етеді. Сервис ЭЦҚ кілттерін, негізгі жеткізгіштердегі негізгі ақпараттың жазбаларын қалыптастыру, ЭЦҚ-ны тексеру кілттерінің сертификаттарын дайындауға және

олардың мәртебесін өзгертуге сұрау салулар дайындау және өңдеу, ЭЦҚ-ны тексеру кілттерінің сертификаттарын және күші жойылған сертификаттардың тізімдерін жасау үшін пайдаланылады.

Ақпаратты қорғау жүйесі КО техникалық құралдарында, оның ішінде резервтік көшіру кезінде өңделетін және сақталатын құпия ақпаратты қорғауды, соның ішінде криптографиялық қорғауды қамтамасыз етеді.

ЭЦҚ құралдары ЭЦҚ кілттерінің жұптарын генерациялау, негізгі ақпаратты сақтау, ЭЦҚ-ны тексеру, ЭЦҚ-ны генерациялау, қол қойылатын және тексерілетін ақпаратты көрсету функцияларын қамтамасыз етеді.

Көрсетілген қызметтерді қамтамасыз ету үшін СҮТ қызметінің КО-сында бір немесе бірнеше адам орындауы мүмкін мынадай сенім білдірілген рөлдер бөлінеді:

СҮТ қызметі КО-сының басшысы – СҮТ қызметі КО-сының жұмысын жалпы ұйымдастыруды жүзеге асырады, СҮТ қызметі КО-сының жұмыс істеуі саласындағы нормативтік актілерді әзірлеу және жетілдіру, ЭЦҚ құралдарын пайдалану жөніндегі жұмысты ұйымдастырады;

СҮТ қызметі КО-сының уәкілетті адамы (сертификаттау әкімшісі) – СҮТ қызметі КО-сының ЭЦҚ кілтін сақтауды және пайдалануды қамтамасыз етеді, СҮТ қызметі КО-сының нормативтік базасын әзірлеуге және ЭЦҚ құралдарын пайдалануға қатысады, Комиссияның СҮТС-ін олардың қажеттілігіне сәйкес сертификаттармен қамтамасыз ету жоспарларын әзірлейді, даулы жағдайларды шешу жөніндегі жұмысты ұйымдастырады, сертификаттар иелерінің өтініштері бойынша электрондық құжаттардағы ЭЦҚ-ның түпнұсқалылығын растау, ЭЦҚ-ны тексеру кілттерінің жасалған сертификаттарындағы СҮТ қызметінің КО-сы уәкілетті адамының ЭЦҚ-сының түпнұсқалылығын растау рәсімдерін жүргізеді;

СҮТ қызметінің КО-сы ақпараттық қауіпсіздігінің әкімшісі, оның лауазымдық міндеттеріне АКҚҚ пайдалану жөніндегі жұмыстарды ұйымдастыру, пайдаланушыларға арналған нұсқаулықтар әзірлеуге қатысу, АКҚҚ-дағы нұсқаулықтар мен қажетті құжаттаманы жеткізуді қамтамасыз ету (оның ішінде орнатылған АКҚҚ БҚ бүтіндігін мерзімдік бақылауды ұйымдастыру), олардың талаптарының орындалуын бақылау кіреді.

Куәландырушы орталықтың құралдарымен мынадай міндетті рөлдер іске асырылады:

жүйелік әкімші, оның өкілеттіктеріне куәландырушы орталықтың серверіндегі және әкімшінің автоматтандырылған жұмыс орнындағы арнайы БҚ-ны әкімшілендіру кіреді:

ақпараттың қорғалуын және қорғау құралдарын теңшеуді қамтамасыз ететін қауіпсіздік әкімшісі;

сертификаттау әкімшісі, оның өкілеттіктеріне ЭЦҚ-ны тексеру кілттерінің сертификаттарын және ЭЦҚ-ны тексеру кілттерінің кері қайтарылған сертификаттарының тізімдерін жасау кіреді;

аудит әкімшісі, оның өкілеттіктеріне жүйелік оқиғаларды және аудит журналдары бойынша ақпаратты қорғау құралдарының оқиғаларын бақылау, сондай-ақ қақтығыстық жағдайларды шешу кіреді.

Бір функционалдық рөл бір немесе бірнеше қызметкерге бекітілуі мүмкін. СҮТ қызметі КО персоналының жалпы саны 2 адамнан кем болмауы шарты сақталған жағдайда, бір қызметкерге бірнеше функционалдық рөл бекітілуі мүмкін.

Комиссия басшылығының шешімі бойынша СҮТ қызметінің КО-сын пайдалану жөніндегі міндеттерді орындайтын қызметкерлердің саны шешілетін міндеттердің көлеміне және күрделілігіне теңбе-тең мөлшерде ұлғайтылуы мүмкін.

III. Ашық кілттер инфрақұрылымына қатысушылардың құқықтары мен міндеттері

3. СҮТ қызметі КО-сының құқықтары мен міндеттері:

СҮТ қызметі КО-сының:

егер өтініш беруші осы Регламентке сәйкес барлық құжаттарды ұсынбаса, құжаттарда толық емес және (немесе) қате ақпарат қамтылса, ұсынылған құжаттардың бұрмалауының айқын белгісі болса, өтінішті қабылдаудан және сертификат шығарудан бас тартуға;

егер олардың көмегімен кілттер және сұрау салу туындаған ЭЦҚ құралдары СҮТ қызметі КО-сының ЭЦҚ құралдарымен үйлеспесе, сертификатқа сұрау салуды қабылдаудан бас тартуға;

егер ЭЦҚ-ның тиісті кілтінің белгіленген қолданылу мерзімі өтіп кетсе, ЭЦҚ-ны тексеру кілтінің сертификатын кері қайтарудан бас тартуға құқығы бар.

СҮТ қызметінің КО-сы:

сертификаттау әкімшісінің ЭЦҚ кілтін шығарылатын сертификаттарда және КСТ-да қалыптастыру үшін ғана пайдалануға;

СҮТ қызметі КО-сы уәкілетті тұлғасының ЭЦҚ кілтінің құпиялылығын қамтамасыз етуге;

КО пайдаланушыларына уәкілетті тұлғаның электрондық құжат нысанындағы ЭЦҚ кілтінің сертификатын ұсынуға;

осы Регламентке сәйкес КСТ-ны өзекті жай-күйде ұстауға;

берілетін сертификаттардың сериялық нөмірлерінің және олардағы ЭЦҚ-ны тексеру кілттерінің бірегейлігін қамтамасыз етуге;

осы Регламентке сәйкес сертификат иесінің сұрау салуы бойынша пайдаланушының сертификатын ең қысқа мерзімді кері қайтаруға;

осы Регламентті КО-ның репозиторийінде қолданыстағы редакцияда жариялауға міндетті.

4. СҮТ қызметінің КО-сын пайдаланушының;

сертификат шығаруға берілетін өтінішпен СҮТ қызметінің КО-сына жүгінуге;

сертификат кері қайтаруға берілетін өтінішпен СҮТ қызметінің КО-сына жүгінуге;

СҮТ қызметінің КО-сы уәкілетті тұлғасының электрондық құжат нысанындағы ЭЦҚ-ны тексеру кілтінің сертификатын алуға;

СҮТ қызметі КО-сының тізілімінен электрондық құжат нысанындағы сертификат алуға;

СҮТ қызметі КО-сының тізілімінен қағаз жеткізгіштегі сертификат алуға;

КО берген сертификаттағы ЭЦҚ-ны тексеру үшін СҮТ қызметінің КО-сына өтініш жасауға;

куәландырушы орталық берген сертификатқа сәйкес келетін кілтті пайдалана отырып қол қойылған құжаттағы ЭЦҚ-ны тексеру үшін СҮТ қызметінің КО-сына өтініш жасауға;

сертификаттардың мәртебелерін тексеру үшін КСТ мен СМТС пайдалануға;

уақыт штамптарын қою үшін КО УШС пайдалануға құқығы бар.

СҮТ қызметінің КО-сын пайдаланушы:

осы Регламентпен танысуға;

меншікті ЭЦҚ кілтінің құпиялылығын қамтамасыз етуге;

ЭЦҚ кілтін оның қолданылу мерзімінің ішінде ғана пайдалануға;

ЭЦҚ кілтін тек тиісті сертификатта көрсетілген саясаттарға сәйкес пайдалануға;

КСТ мен СМТС-ты сертификаттардың мәртебелері туралы ақпарат алу үшін пайдалануға;

ЭЦҚ кілтінің құпиялылығы бұзылған деп санауға негіздемелер болған жағдайда ЭЦҚ кілтін пайдаланбауға;

ЭЦҚ кілтінің компрометациясы жағдайында КО-ны жедел хабардар етуге және сертификатты кері қайтаруды сұрауға;

кілттер жұбын және СҮТ қызметі КО-сының ЭЦҚ құралдарымен үйлесімді ЭЦҚ құралдарының сертификаттарына сұрау салуларды генерациялау үшін пайдалануға;

СҮТ қызметінің КО-сы ЭЦҚ кілттерін жоспардан тыс ауыстыруды жүргізу туралы хабарланған жағдайда СҮТ қызметі КО-сының жаңа түбір сертификатын, жасалған кросс-сертификатты алуға, оларды орнатуды орындауға және СҮТ тиісті серверлерінде кері қайтарудың жергілікті тізімдерін жаңартуды жүзеге асыруға міндетті.

IV. СҮТ қызметінің КО қызметтерін көрсету үшін қажетті рәсімдерді (әрекеттерді) орындау тәртібі және мерзімдері

5. Қызметтердің құны

СҮТ қызметінің КО-сы СҮТ қызметінің функцияларын қамтамасыз ету үшін өтеусіз негізде сертификаттар шығаруды жүзеге асырады.

6. Негізгі жеткізгіштердің тізбесі

СҮТ қызметінің КО-сы негізгі жеткізгіштер ретінде:

ЕЭК Алқасының 29.08.17 ж. № 101 ҚБПҮ шешімімен бекітілген қатерлер моделіне сәйкес ЭЦҚ-ның сенім білдірілген есептеу құрылғысын (СЕҚ) (ақпарат СЭҚ құрамындағы SSD-дискіде сақталады);

негізгі жеке жеткізгіштерді – арнайы дайындалған USB-flash жеткізгіштерді пайдаланады.

ЭЦҚ кілтін инициализациялау үшін қажетті негізгі ақпараттың бір бөлігі СЕҚ-та, ал екінші бөлігі USB-flash жеткізгіште сақталады. СЕҚ-тағы және USB-flash жеткізгіштердегі ақпарат қорғалған түрде сақталады.

Кілттерді инициализациялау және ЭЦҚ кілттерімен жұмыс ЭЦҚ СЕҚ-ында ғана және тиісті USB-flash жеткізгіш ұсынылған және ЭЦҚ кілтінің иесі сәтті аутентификацияланған жағдайда ғана орындалады.

7. СҮТ қызметі КО-сының ЭЦҚ кілттерін жоспардан тыс ауыстыру тәртібі

СҮТ қызметі КО-сының ЭЦҚ кілттерін жоспардан тыс ауыстыру пайдаланылатын ЭЦҚ құралдарының талаптарына сәйкес ерте дегенде КО-ның ЭЦҚ кілттерінің қолданысы басталған сәттен бастап 1 жыл өткеннен кейін және 1 жыл және 3 айдан кешіктірілмей орындалады.

ЭЦҚ кілтін жоспарлы ауыстыру рәсімі мынадай тәртіппен жүзеге асырылады:

СҮТ қызметі КО-сының сертификаттау әкімшісі СҮТ қызметі КО-сының ақпараттық қауіпсіздік әкімшісімен бірлесіп ЭЦҚ-ның жаңа кілтін және соған сәйкес келетін ЭЦҚ-ны тексеру кілтін қалыптастырады;

СҮТ қызметі КО-сының өздігінен қол қойылған сертификаты қалыптастырылады және сертификаттар тізілімінде сақталады;

сертификат алмалы-салмалы жеткізгіште сақталады және СҮТ қызметі КО-сының серверіне орнатылады.

СҮТ қызметінің КО-сы ЭЦҚ-сының өзекті емес кілті СҮТ қызметінің КО-сы өзінің жұмыс істеу кезеңінде шығарған электрондық нысандағы кері қайтарылған сертификаттардың тізімдерін қалыптастыру үшін ғана пайдаланылады.

СҮТ қызметінің КО-сы ЭЦҚ-сының кілттерін жоспарлы ауыстыру туралы пайдаланушыларды хабардар ету СҮТ қызметі КО-сының жаңа сертификатын СҮТ қызметі КО-сының репозитоийінде жариялау жолымен жүзеге асырылады.

8. СҮТ қызметі КО-сының электрондық қолтаңба кілттерін жоспардан тыс ауыстыру тәртібі

СҮТ қызметінің КО-сы ЭЦҚ-сының кілттерін жоспардан тыс ауыстыру СҮТ қызметі КО ЭЦҚ-ның кілті компрометацияланған жағдайда немесе ЭЦҚ құралдары аппараттық бөлігінің (СЕҚ және (немесе) USB-flash жеткізгіш) физикалық

жарамсыздығы туындаған жағдайда не ЭЦҚ құралдарын пайдаланудың мүмкін еместігіне әкеп соқтыратын бағдарламалық қамтамасыз етудің іркілісі кезінде орындалады.

СҮТ қызметі КО-сының ЭЦҚ-сы кілтінің компрометациясына күдік болмаған кезде кілтті ауыстыру осы Регламенттің 7-тармағында көрсетілген кілттерді жоспарлы ауыстыру тәртібіне сәйкес орындалады.

ЭЦҚ кілтінің компрометациясы (немесе оның компрометациясына күдік болуы) кезінде оны ауыстыру рәсімі мынадай тәртіппен жүзеге асырылады:

СҮТ қызметі КО-сының сертификаттау әкімшісі СҮТ қызметі КО-сының ақпараттық қауіпсіздік әкімшісімен бірлесіп кілттердің жаңа жұбын әзірлейді және осы Регламенттің 7-тармағында көрсетілген кілттерді жоспарлы ауыстыру тәртібіне сәйкес жаңа сертификат дайындайды.

СҮТ қызметі КО-сының түбір сертификатының компрометацияланған тиісті кілтіне кросс-сертификаттау орындалады (кросс-сертификатқа СҮТ қызметінің КО-сы ЭЦҚ-сының жаңа кілтімен қол қойылады);

СҮТ қызметі КО-сының компрометацияланған түбір сертификатының күшін жою (кері қайтару) рәсімі орындалады. Кері қайтарылған сертификаттардың қалыптастырылған тізіміне СҮТ қызметінің КО-сы ЭЦҚ-сының жаңа кілтімен қол қойылады.

Сертификаттардың иелерін кілттерді жоспарлы ауыстыру туралы хабардар ету телефон байланысын пайдалана отырып хабарлау жолымен жүргізіледі.

СҮТ қызметінің КО-сы ЭЦҚ-сының кілттерін жоспардан тыс ауыстыру кезінде СҮТ әкімшісі СҮТ қызметі КО-сының жаңа түбір сертификатын, жасалған кросс-сертификаттыалуға, оларды орнатуды орындауға және СҮТ-тің тиісті серверлеріндегі кері қайтарудың жергілікті тізімдерін жаңартуды жүзеге асыруға тиіс.

9. СҮТ қызметі КО-сының сертификаттарды сүйемелдеу жөніндегі әрекеттері

9.1. Сертификат шығаруға өтініш беру

Сертификат шығаруға өтініш қағаз жеткізгіштегі құжат нысанында СҮТ қызметі КО-сына беріледі, оның деректемелерінің түпнұсқалылығы осы Регламентке № 2 қосымшаға сәйкес тексеріледі. Өтініш өтініш берушінің қолтаңбасымен, сондай-ақ ұйымның – сертификат ол үшін сұратылатын тиісті СҮТ операторының мөрімен куәландырылуға тиіс, не осы Регламентке № 3 қосымшаға сәйкес нысан бойынша мүше мемлекеттің заңнамасына сай нотариалды куәландырылуға тиіс.

Ұйымдардың – СҮТ қызметі сервистері операторларының тізбесі Комиссияның шешімімен айқындалады.

СҮТ түпнұсқалылығын растау сервисінің сертификатын және СҮТ уақыт штамптары қызметінің сертификатын шығаруға өтінішті ұйымның – СҮТ операторының уәкілетті қызметкерлері ғана бере алады.

СҮТ түпнұсқалылығын растау сервисінің (ТРС) сертификатын және СҮТ уақыт штамптары қызметінің сертификатын шығаруға өтініштерді беру кезінде ұйымның – СҮТ операторының уәкілетті қызметкері СҮТ-те СҮТ сервистерінің негізгі және резервтік серверлерінің болуын ескереді. СҮТ қызметінің КО-сында бір СҮТ-ті сервистер сертификаттарымен қамтамасыз ету үшін 4 өтініш беріледі:

СҮТ негізгі серверінің ТРС үшін;

СҮТ резервтік серверінің ТРС үшін;

СҮТ негізгі серверінің УШС үшін;

СҮТ резервтік серверінің УШС үшін.

Өтініш беруші СҮТ сервистерінің ЭЦҚ-ны тексеру кілттерінің сертификаттарын шығаруға өтініштерді СҮТ қызметінің КО-сына өтініш беруші тиісті СҮТ серверінде тікелей туындатқан иеліктен шығарылатын жеткізгіштегі (CD немесе DVD дискідегі) ЭЦҚ-ны тексеру кілтінің сертификатына PKCS#10 форматындағы сұрау салулар файлдарын ұсынады.

ЭЦҚ кілттерін ауыстыру кезінде, егер өтініш беруші адам өзгермеген жағдайда, сертификат шығаруға сұрау салу файлы бар жеткізгішті СҮТ қызметінің КО-сына жөнелту жолымен Комиссияға бармастан өтінішті оңайлатып беруге жол беріледі (ЭЦҚ кілтінің компрометациялануы жағдайларынан басқа). Комиссияға өзі бармастан СҮТ қызметінің КО-сына берілетін сертификат шығаруға сұрау салуларға СҮТ-тің тиісті кіші жүйесінің түпнұсқалылығын растау сервисі ЭЦҚ-сының қолданыстағы кілтімен қол қойылуға тиіс.

9.2. Сертификат шығаруға берілетін өтінішті өңдеу

Өтініш беруші сәтті аутентификацияланғаннан кейін сертификаттау әкімшісі СҮТ қызметі КО-сының ақпараттық қауіпсіздік әкімшісімен бірлесіп сәйкестендіру ақпаратының сертификат шығаруға өтініштегі деректерге сәйкестігін тексереді. Сертификат шығаруға сұрау салу дерекқорда сақталады. Бастапқы тіркеу кезінде сәйкестендіру ақпараты да дерекқорға енгізіледі және сертификатты кері қайтаруға телефонмен сұрау салу кезінде жедел аутентификациялау үшін өтініш берушіге пароль сөзі беріледі.

Сертификат шығаруға өтініш, егер мынадай талаптар орындалған:

өтініш беруші осы Регламенттің 23.2-тармағына сәйкес аутентификациялау рәсімінен өткен;

сертификат сұрату файлы белгіленген форматқа (сұрау салудың форматы осы Регламентке № 1 қосымшада көрсетілген) сәйкес келген, сұрау салудағы сәйкестендіру деректері қағаз жеткізгіштегі өтініште көрсетілген деректермен үйлескен;

сұрау салудағы DN бірегей аты осы Регламенттің 23.1.1-тармағының талаптарына сәйкес келген;

кілттерді генерациялау алгоритмі және сұрау салу қолтаңбалары СҮТ қызметінің КО-сында пайдаланылатындармен үйлескен жағдайда өңдеуге беріледі.

Егер келтірілген талаптардың ең болмағанда бірі орындалмаса, онда сертификат шығаруға берілетін өтініш міндетті түрде өтініш берушіге хабарлана отырып қабылданбайды.

9.3. Сертификат шығаруға берілетін өтінішті өңдеу мерзімі

Сертификат шығаруға берілетін өтінішті өңдеу 1 жұмыс күнінің ішінде жүргізіледі. Егер СҮТ қызметінің КО-сына өтініш берушіні аутентификациялау үшін қосымша деректер талап етілген жағдайда, өңдеу мерзімі ұзартылуы мүмкін.

10. Сертификат шығару

10.1. СҮТС серверінің сертификатын шығару

СҮТС серверінің сертификатын шығару кезінде өтініш беруші СҮТ қызметінің КО-сына өтініш беруші тікелей СҮТС серверінде генерациялаған белгіленген форматтағы сұрау салу файлын ұсынады. СҮТ қызметі КО-сының сертификаттау әкімшісі СҮТ қызметі КО-сының дерекқорындағы өтініштен сәйкестендіру ақпаратының болуын тексереді және "СҮТС сервері" шаблоны бойынша сұрау салу файлының негізінде сертификат шығаруды жүзеге асырады.

Сертификаттардың қалыптары осы Регламентке № 1 қосымшада келтірілген.

10.2. СМТС серверінің сертификатын шығару

СМТС серверінің сертификатын шығару кезінде өтініш беруші СҮТ қызметінің КО-сына өтініш беруші тікелей СМТС серверінде генерациялаған белгіленген форматтағы сұрау салу файлын ұсынады. СҮТ қызметі КО-сының сертификаттау әкімшісі СҮТ қызметінің дерекқорындағы өтініштен сәйкестендіру ақпаратының болуын тексереді және "СМТС сервері" шаблоны бойынша сұрау салу файлының негізінде сертификат шығаруды жүзеге асырады.

Сертификаттардың қалыптары осы Регламентке № 1 қосымшада келтірілген.

10.3. УШС серверінің сертификатын шығару

УШС серверінің сертификатын шығару кезінде өтініш беруші СҮТ қызметінің КО-сына өтініш беруші тікелей УШС серверінде генерациялаған белгіленген форматтағы сұрау салу файлын ұсынады. СҮТ қызметі КО-сының сертификаттау әкімшісі КО дерекқорындағы өтініштен сәйкестендіру ақпаратының болуын тексереді және "УШС сервері" шаблоны бойынша сұрау салу файлының негізінде сертификат шығаруды жүзеге асырады.

Сертификаттардың шаблондары осы Регламентке № 1 қосымшада келтірілген.

10.4 Меншік иесін сертификаттың шығарылуы туралы хабардар ету

Уәкілетті өкілі КО-ға жеке өзі келуі кезінде берген СҮТ операторынан келіп түскен сұрау салу бойынша сертификаттар шығарылғаннан кейін СҮТ қызметі КО-сының әкімшісі оператордың өкіліне қағаз жеткізгіштегі сертификатты және алмалы-салмалы жеткізгіштегі электрондық түрдегі сертификатты беру жолымен меншік иесін сертификаттың шығарылғаны туралы хабардар етеді.

Уәкілетті өкілінің КО-ға жеке келуінсіз берілген СҮТ операторынан келіп түскен сұрау салу бойынша сертификаттар шығарылғаннан кейін СҮТ қызметі КО-сының әкімшісі телефон байланысы арқылы не шығарылған электрондық түрдегі сертификатты қоса бере отырып, пошта хабарламасын жөнелту арқылы меншік иесін сертификаттың шығарылғаны туралы хабардар етеді. Сертификат иесінің мекенжайына қағаз жеткізгіштегі сертификат қосымша жіберіледі.

11. Иесінің сертификатты қабылдауы

11.1. Сертификатты қабылдауды растау

Сертификаттың иесіне сертификатпен бірге қағаз құжат нысанындағы сертификат беріледі. Меншік иесі сертификатты қабылдап алу кезінде сертификаттың құрамына енгізілген сәйкестендіру ақпаратымен танысуға міндетті. Егер сәйкестендіру ақпараты дұрыс болған жағдайда, меншік иесі қағаз жеткізгіштегі сертификатты өз қолтаңбасымен куәландырады. Қағаз жеткізгіштегі сертификаттың бір данасы иесіне беріледі, екінші данасы СҮТ қызметінің КО-сына мұрағаттық сақтауға беріледі.

Қағаз жеткізгіштегі құжат нысанындағы сертификатқа қол қойылу фактісі сертификатты қабылдауды растау болып табылады.

11.2. Сертификатты жариялау

Берілген сертификат СҮТ қызметі КО-сының серверінде жарияланады.

11.3. Сертификатты жасау және беру мерзімі

Сертификатты жасау және беру мерзімі өтініш пен растау құжаттары берілген сәттен бастап бір жұмыс күнінен аспайды.

12. Кілттер мен сертификаттарды пайдалану

Кілттер мен сертификаттарды пайдалану мақсаттары сертификат оған сәйкес берілген саясатқа байланысты болады.

12.1. СҮТС серверінің кілті және сертификаты

СҮТС серверінің ЭЦҚ кілті ЭЦҚ-ны тексеру түбіртектерінде және ұлттық сегменттердің СҮТС автоматты режимде тексеру жүргізуге сұрау салуларда ЭЦҚ қалыптастыру үшін ғана пайдаланылады.

СҮТС серверінің сертификаты түбіртектердің және сұрау салулардың құрамына енгізіледі және осы түбіртектер мен сұрау салуларда ЭЦҚ-ны тексеру, сондай-ақ СҮТС серверін сәйкестендіру үшін пайдаланылады.

12.2. СМТС серверінің кілті және сертификаты

СМТС серверінің ЭЦҚ кілті қызметтің OCSP-жауаптарында автоматты режимде сенім білдірілген жауапкер режимінде ЭЦҚ қалыптастыру үшін ғана пайдаланылады.

СМТС сертификаты сервистің OCSP-жауабының құрылымына енгізіледі және OCSP-жауаптағы ЭЦҚ-ны тексеру және СМТС сәйкестендіру үшін пайдаланылады.

12.3. УШС серверінің кілті және сертификаты

СҮТС сұрау салулары жөніндегі қызмет беретін уақыт штамптарында ЭЦҚ қалыптастыру үшін ғана пайдаланылады.

СҮТС сертификатын сервис сервері берілетін уақыт штамптары құрылымына енгізеді және уақыт штамптарындағы ЭЦҚ-ны тексеру және қызметті сәйкестендіру үшін пайдаланылады.

13. Сертификатты жаңарту

Сертификатты жаңарту қолданыстағы кілттер жұбы үшін жүргізілмейді. Әрбір сертификат кілттердің жаңа жұбымен шығарылады.

14. Кілттерді жаңарту

Кілттерді жаңарту сертификаттың иесі тіркеген кілттердің жаңа жұбы үшін жаңа сертификат беруді білдіреді. Жаңа кілттері бар сертификатты сәйкестендіру және шығару рәсімдері бастапқы тіркеу рәсімдеріне ұқсас және олар осы Регламенттің 23.2-тармағына сәйкес орындалады.

15. Сертификатқа енгізілетін деректерді өзгерту

СҮТ қызметінің КО-сы сертификаттарды өзгертуді жүргізбейді. Сертификатқа енгізілетін сәйкестендіру деректері өзгерген жағдайда осы Регламенттің 20.2-тармағына сәйкес жаңа кілттер жұбы бар жаңа сертификат шығару жүргізіледі.

16. Сертификатты кері қайтару және оның қолданысын тоқтата тұру

16.1. Сертификатты кері қайтару үшін негіздемелер

СҮТ қызметінің КО-сы берген ЭЦҚ-ны тексеру кілтінің сертификаты осы Регламенттің 30.3-тармағына сәйкес ЭЦҚ кілтінің компрометациясы жағдайында, сондай-ақ сертификатқа енгізілетін ақпарат дәл болмаған немесе толық болмаған жағдайда кері қайтаруға жатады.

Сертификаттың қолданысын тоқата тұру қолдау таппайды.

16.2. Сертификатты кері қайтаруға сұрау салу

СҮТ қызметінің КО-сы берген сертификатты кері қайтаруды сертификаттың иесі немесе СҮТ қызметі КО-сының басшысы жазбаша нысанда сұратуы мүмкін.

16.3. Сертификатты кері қайтаруға сұрау салуды беру

Сертификатты кері қайтаруға сұрау салу CD/DVD оптикалық алмалы-салмалы жеткізгіші пайдаланыла отырып СҮТ қызметінің КО-сына берілуі мүмкін. Бұл ретте сұрау салуға СҮТ қызметінің КО-сы берген кері қайтарылатын сертификаттың кілті пайдаланыла отырып қол қойылады. Кері қайтаруға сұрау салу СҮТ қызметінің КО-сына бастапқы тіркеу кезінде тағайындалатын парольдік сөз бойынша сертификат иесінің аутентификациялануымен телефон байланысы бойынша да берілуі мүмкін.

Кері қайтаруға сұрау салу СҮТ қызметінің КО-сына берілгеннен кейін сертификаттың иесі сертификат иесінің өз қолтаңбасымен, уәкілетті адамның қолтаңбасымен және СҮТ операторы органының (ұйымының) мөрімен куәландырылған не ұлттық заңнамаға сәйкес нотариалдық куәландырылған қағаз жеткізгіштегі сертификатты кері қайтаруға өтініш беруге тиіс. Өтініштің нысаны осы Регламентке № 4 қосымшада келтірілген.

16.4. Сертификатты кері қайтаруға сұрау салуды өңдеуді кешіктірудің жол берілетін мерзімдері

Сертификатты кері қайтаруға сұрау салу 1 жұмыс күнінің ішінде өңделеді.

17. Сенім білдіруші тарап сертификатының мәртебесін тексеруге қойылатын талаптар

Сенім білдіруші тарап ЭЦҚ-мен электрондық құжатты алғаннан кейін сертификаттардың мәртебелерін тексеру хаттамасы бойынша ЭЦҚ-ны тексеру кілтінің сертификатын кері қайтарылған сертификаттардың тізімі бойынша жедел режимде тексеруге міндетті. Егер құжаттың ЭЦҚ-сы оның көмегімен тексерілетін сертификат кері қайтарылған сертификаттардың тізілімінде болса, онда мұндай құжатты сенім білдіруші тарап қабылдамайды.

17.1. КСТ шығару жиілігі

Кері қайтарылған сертификаттардың тізімін СҮТ қызметінің КО-сы сертификатты кері қайтаруға сұрау салу өңделгеннен кейін дереу, бірақ 3 айда 1 реттен сиретпей (тіпті тізімде өзгерістер болмаған кезде де) шығарады және репозиторийге мына мекенжайлар бойынша жариялайды:

http:// <XXX>00.DTS.EEC;

http:// <XXX>01.DTS.EEC.

17.2. КСТ жариялауды кешіктірудің ең ұзақ уақыты

Кері қайтарылған сертификаттардың тізімі СҮТ қызметі КО-сының серверінде тікелей шығарудан кейін жарияланады. Жариялауды кешіктірудің ең ұзақ уақыты 1 сағатты құрайды.

17.3. Сертификаттарды нақты уақыт режимінде тексеру сервисі

СҮТ қызметінің КО-сы сертификаттарды нақты уақыт режимінде тексеру қызметтерін көрсетеді. Осы түрдегі қызмет RFC 6960-та сипатталған OCSP хаттамасы бойынша көрсетіледі.

OCSP хаттамасы сертификаттың мәртебесі туралы ақпаратты CRL толық тізімін алу және тексеру қажеттігінсіз алуға мүмкіндік береді.

OCSP хаттамасы сұрау салу – жауап моделінің негізінде әрекет етеді. СҮТ қызметі КО-сының құрылымына кіретін СМТС сервері әрбір сұрау салудың жауабына сертификаттың мәртебесі туралы мынадай стандарттық ақпарат жібереді:

дұрыс (ағылш. good) – сұрау салуға оң жауапты білдіреді, оны сертификаттың жарамды болып табылатындығын куәландыру ретінде бір мәнді түсіндіру қажет;

кері қайтарылған (ағылш. revoked) – сертификаттың кері қайтарылғанын білдіреді;

белгісіз (ағылш. unknown) – тексерілетін сертификатты СҮТ қызметінің КО-сы бермегенін білдіреді.

OCSP сервисі СҮТ қызметі КО-сының КСТ-ын негізге ала отырып жауап дайындайды.

18. Кілттердің компрометацияланған жұбын ауыстыру кезіндегі ерекше талаптар

Кілттер компрометацияланған жағдайда тиісті сертификат дереу КСТ-ға енгізіледі және жаңа сертификат беру бастапқы тіркеу үшін көзделген тәртіппен жүргізіледі.

19. Сертификаттар қолданысын тоқата тұрудың негіздемелері

СҮТ КО-сы берілген сертификаттардың қолданысын тоқата тұрмайды.

20. Сертификаттардың мәртебелері қызметтері

20.1. СҮТ қызметінің КО-сы берген сертификаттардың мәртебесі туралы хабардар ету тәсілдері

СҮТ қызметінің КО-сы берген сертификаттардың мәртебесі туралы ақпаратты СҮТ қызметі КО-сының репозиторийінде жарияланатын КСТ негізінде, сондай-ақ OCSP хаттамасы бойынша алуға болады. OCSP қызметінің серверіне қол жеткізу туралы ақпарат берілген әрбір сертификатта қамтылады.

20.2. Сервистің қол жетімділігі

Сертификат мәртебесін тексеру жөніндегі қызметтер тәулігіне 24 сағат, аптасына 7 күн қол жетімді болады.

21. Кілттерді депозиттеу және қалпына келтіру

СҮТ қызметінің КО-сы кілттерді депозиттеуді және қалпына келтіруді жүзеге асырмайды.

22. Репозиторий

Репозиторий СҮТ қызметі КО-сының серверіне орналастырылған файлдар мен каталогтардың жиынтығы болып табылады. Репозиторийде сертификаттар, кері қайтарылған сертификаттардың тізімдері және осы Регламент болады.

СҮТ қызметінің КО-сы өзінің Репозиторийінде жариялаған барлық ақпарат мына мекенжайлар бойынша қол жетімді болады:

http://<XXX>00.DTS.EEC,

http:// <XXX>01.DTS.EEC

Репозиторий мынадай ақпаратты:

СҮТ қызметінің КО-сы берген барлық сертификаттарды;

кері қайтарылған сертификаттардың өзекті тізімдерін;

СҮТ қызметі КО-сының басшысы бекіткен сертификаттарды басқару саясаттарын;

осы Регламенттің өзекті нұсқасын қамтиды.

Репозиторийдегі ақпарат мынадай кезеңділікпен:

СҮТ қызметінің КО-сы берген сертификаттар – тікелей жаңа сертификат шығарылғаннан кейін;

кері қайтарылған сертификаттардың тізімдері – кемінде 3 айда 1 рет және бұрын берілген сертификаттар кері қайтарылған жағдайда шұғыл;

осы Регламенттің жаңа нұсқасы – оның бекітілу фактісі бойынша жарияланады.

СҮТ қызметінің КО-сы репозиторийге рұқсатсыз қосудың, жоюдың немесе ондағы жазбаларды өзгертудің алдын алатын қорғау механизмдерін пайдаланады.

Репозиторийге қол жетімділік тәулігіне 24 сағат, аптасына 7 күн қамтамасыз етіледі.

КО орналастырылған сертификаттарға және http хаттамасы бойынша КСТ-ға қол жетімділікті шектемейді.

23. Сәйкестендіру және аутентификациялау тәртібі

23.1. Сертификаттың құрамына енгізілетін сәйкестендіру ақпаратына қойылатын талаптар

23.1.1. Атаулардың түрлері

Сертификаттарда көрсетілетін сертификаттар иелерінің сәйкестендіру деректері, сондай-ақ СҮТ қызметі КО-сының сәйкестендіру деректері X.500 Ұсынымдарына сәйкес кодталған айырымдық атауды (DN) білдіруге тиіс. Айырымдық атау СҮТ қызметі КО-сының шеңберінде бірегей болуға тиіс.

Айырымдық атау құрамдастарының құрамы мен форматы X.501 ұсынымдарына сәйкес болуға тиіс.

Атау құрамдастарына (сертификат иесінің сәйкестендіру ақпаратына) қойылатын талаптар 1-кестеде келтірілген.

1-кесте

Атрибут	Талаптар

Distinguished name (DN)	айырымдық атау СҮТ қызметі PKI шеңберінде бірегей болуға тиіс
Country (C)	МЕМСТ 7.67-2003 (ИСО 3166-1:1997) сәйкес елдің екі символдық коды
Organization (O)	жарғылық құжаттарға сәйкес ұйымның қысқартылған атауы
Description	ұйымның жалпы атауы
StateOrProvinceName(S)	СҮТ ұйымы-операторы тіркелген ұйымның орналасқан саласы
LocalityName (L)	СҮТ ұйымы-операторы тіркелген елді мекеннің атауы
StreetAddress	СҮТ ұйымы-операторы орналасқан мекенжай
Ақпараттық жүйенің сәйкестендіргіші	
E-Mail Address (E)	СҮТ ұйымы-операторы өкілінің, қызметтің немесе сервистің электрондық поштасының мекенжайы немесе сертификаттау әкімшісі электрондық поштасының мекенжайы
CommonName (CN)	өрісінің мәні сертификат соған сәйкес берілген саясатқа байланысты: <СҮТ псевдонимі> – СҮТС серверінің сертификаты (мысалы, интеграциялық сегменттің СҮТС-і) <СМТС ИС> – сертификат мәртебесін тексеру сертификаты <УШС псевдонимі> – уақыт штамптары қызметінің сертификаты <тегі, аты, әкесінің аты> – әкімшінің немесе оператордың сертификаты

DN атауын СҮТ қызметінің КО-сына өтініш беретін адам ұсынады. Егер осы атау жалпы талаптарға сәйкес келсе және бірегей болып табылса, яғни СҮТ қызметінің КО-сында тіркеліп қойған сертификаттың басқа иесінің DN-на сәйкес келсе, онда ол сәйкестендіру деректері ретінде қабылданады және сертификат иесін тіркеу кезінде СҮТ қызметінің КО-сына енгізіледі.

DN атауының бірегейлігін қамтамасыз ету үшін СҮТ қызметі КО-сының операторлары айырымдық атаудың CN құрамдасына әртүрлі символдар қосуы мүмкін.

23.1.2. Анонимдік сертификаттар

СҮТ қызметінің КО-сы анонимдік сертификаттар шығармайды. Псевдонимдер ретінде қызметтер мен сервистердің атаулары пайдаланылады.

23.2. СҮТ қызметінің КО-сын пайдаланушыларды сәйкестендіру және аутентификациялау және бастапқы тіркеу рәсімдері

СҮТ қызметінің КО-сын пайдаланушыларды тіркеу сертификаттар шығаруға өтініш берген жеке тұлғаның СҮТ қызметінің КО-сы берген бір де бір жарамды сертификаты болмаған кезде жүзеге асырылады.

Ұсынылған деректер сәтті тексерілгеннен кейін өтініш беруші СҮТ қызметінің КО-сын уәкілетті пайдаланушылар тізіміне енгізеді және кері қайтаруға сұрау салу

кезінде жедел сәйкестендіру үшін пароль сөзін алады. Сертификат шығаруға берілетін өтініш өңделеді және сертификатты шығару жүзеге асырылады.

Сәйкестендіру рәсімі СҮТ қызметі КО-сының басшысы бекіткен сертификаттар саясаттарымен айқындалады.

23.2.1. СҮТ түпнұсқалылығын растау сервисі серверінің сертификатын сұрату кезіндегі сәйкестендіру және аутентификациялау тәртібі

Сертификат шығаруға өтініш беру кезінде өтініш берушіні сәйкестендіру СҮТ қызметінің КО-сына жеке өтініш жасау кезінде ғана жүзеге асырылады. Өтініш беруші мынадай құжаттарды ұсынуға тиіс:

қағаз жеткізгіштегі сертификат шығаруға өтініш;

сертификатқа өтінім беретін жеке адамның паспорты;

СҮТ ұйымы-операторы өтініш берушінің атына берген сертификат алу құқығына сенімхат;

СҮТ бағдарламалық-аппараттық кешенін (бұдан әрі – БАК) пайдалануға жауапты адамды тағайындау туралы ұйым басшысы куәландырған ұйым бойынша бұйрықтың көшірмесі немесе бұйрықтан үзінді.

Егер өтініш берушінің жеке басын куәландыратын паспорт түпнұсқа болып табылса және құжаттағы фотосурет ұсынушының фотосуреті болып табылса, ал өтініш беруші СҮТ уәкілетті тұлғаларының тізіміне (бұған дейін СҮТ операторы электрондық поштамен ұсынған) кірген болса, онда өтініш беруші аутентификацияланған болып есептеледі.

Егер ұйымның сенімхаттағы қолтаңбалары мен мөрлері және бұйрықтың (үзіндінің) көшірмелері түпнұсқа болып табылса (не сенімхат ұлттық заңнамаға сәйкес нотариалды куәландырылса), ал сенімхатты берген ұйым СҮТ ұйымдары-операторларының тізбесіне кірген болса, өтініш берушінің өкілеттіктері расталған болып есептеледі.

Құжаттардың түпнұсқалылығын тексеру осы Регламентке № 2 қосымшаға сәйкес жүргізіледі.

23.2.2. Сертификаттың мәртебесін тексеру сервисінің сертификатын сұрату кезіндегі сәйкестендіру және аутентификациялау тәртібі

Сертификат шығаруға өтініш беру кезінде өтініш берушіні сәйкестендіру СҮТ қызметінің КО-сына жеке өтініш жасау кезінде ғана жүзеге асырылады. Өтініш беруші мынадай құжаттарды ұсынуға тиіс:

қағаз жеткізгіштегі сертификат шығаруға өтініш;

сертификатқа өтінім беретін жеке адамның паспорты;

СҮТ қызметі КО-сының ұйымы-операторы өтініш берушінің атына берген СМТС сертификатын алу құқығына сенімхат;

СМТС пайдалануға жауапты адамды тағайындау туралы ұйым басшысы куәландырған ұйым бойынша бұйрықтың көшірмесі немесе бұйрықтан үзінді.

Егер өтініш берушінің жеке басын куәландыратын паспорт түпнұсқа болып табылса және құжаттағы фотосурет ұсынушының фотосуреті болып табылса, онда өтініш беруші аутентификацияланған болып есептеледі.

Егер ұйымның бұйрықтың көшірмесіндегі (үзіндідегі) қолтаңбалары мен мөрлері түпнұсқа болып табылса (не сенімхат ұлттық заңнамаға сәйкес нотариалды куәландырылса), ал сенімхатты берген ұйым СҮТ ұйымдары-операторларының тізбесіне кірген болса, өтініш берушінің өкілеттіктері расталған болып есептеледі.

Құжаттардың түпнұсқалылығын тексеру осы Регламентке № 2 қосымшаға сәйкес жүргізіледі.

23.2.3. Уақыт штамптары сервисінің сертификатын сұрату кезіндегі сәйкестендіру және аутентификациялау тәртібі

УШС сертификатын шығаруға өтініш беру кезінде өтініш берушіні сәйкестендіру СҮТ қызметінің КО-сына жеке өтініш жасау кезінде ғана жүзеге асырылады. Өтініш беруші мынадай құжаттарды ұсынуға тиіс:

қағаз жеткізгіштегі сертификат шығаруға өтініш;

сертификатқа өтінім беретін жеке адамның паспорты;

СҮТ операторы өтініш берушінің атына берген УШС сертификатын алу құқығына сенімхат;

УШС (немесе СҮТ БАК) пайдалануға жауапты адамды тағайындау туралы ұйым басшысы куәландырған ұйым бойынша бұйрықтың көшірмесі немесе бұйрықтан үзінді.

Егер өтініш берушінің жеке басын куәландыратын паспорт түпнұсқа болып табылса және құжаттағы фотосурет ұсынушының фотосуреті болып табылса, онда өтініш беруші аутентификацияланған болып есептеледі.

Егер ұйымның сенімхаттағы, бұйрықтың көшірмесіндегі (үзіндідегі) қолтаңбалары мен мөрлері түпнұсқа болып табылса (не сенімхат ұлттық заңнамаға сәйкес нотариалды куәландырылса), өтініш беруші УШС (СҮТ БАК) пайдалануға жауапты болып тағайындалса, ал ұйым УШС (СҮТ БАК) операторы болып табылса, өтініш берушінің өкілеттіктері расталған болып есептеледі.

Құжаттардың түпнұсқалылығын тексеру осы Регламентке № 2 қосымшаға сәйкес жүргізіледі.

23.2.4. Кілттерді жаңарту кезіндегі сәйкестендіру және аутентификациялау

Кілттерді жоспарлы ауыстыру кезінде сертификат шығаруға өтініш беру кезіндегі сәйкестендіру және аутентификациялау сертификаттың саясатына қарай осы Регламенттің осы тармағында сипатталған бастапқы сәйкестендірудің ұқсас тәртібіне сәйкес жүргізіледі.

23.2.5. Сертификат кері қайтарылғаннан кейін сұрау салу беру кезіндегі сәйкестендіру және аутентификациялау

Сертификат кері қайтарылғаннан кейін сұрау салу беру кезіндегі сәйкестендіру және аутентификациялау сертификаттың саясатына қарай осы Регламенттің осы тармағында сипатталған бастапқы сәйкестендірудің ұқсас тәртібіне сәйкес жүргізіледі.

23.2.6. Сертификатты кері қайтару кезіндегі сәйкестендіру және аутентификациялау

Кері қайтаруға сұрау салу беру кезіндегі аутентификациялау бастапқы тіркеу процесінде берілетін парольдік сөз бойынша жүзеге асырылады. Кері қайтаруға сұрау салуды жедел өңдеу үшін сертификаттың иесі СҮТ қызметінің КО-сына өтініш жасау кезінде өзінің атын, тегін, лауазымын және парльдік сөзді атауға тиіс.

Егер СҮТ қызметі КО-сының дерекқорындағы сертификат иесінің сәйкестендіру деректері және берілген парольдік сөзі өтініш беру кезінде көрсетілгендермен сәйкес келсе, онда сертификаттың иесі аутентификацияланған болып есептеледі және кері қайтаруға сұрау салу өңдеуге беріледі.

Кері қайтаруға өтініш алмалы-салмалы жеткізгіш пайдаланыла отырып берілген жағдайда пайдаланушының аутентификациясы сұрау салудың ЭЦҚ-ны тексеру кілті арқылы жүзеге асырылады.

Егер сертификат иесінің сәйкестендіру деректері СҮТ қызметі КО-сының дерекқорында қамтылса және хабардағы ЭЦҚ дұрыс болса, онда пайдаланушы аутентификацияланған болып есептеледі және сұрау салу өңделеді.

24. Қауіпсіздікті қамтамасыз етудің физикалық, ұйымдастыру және пайдалану шаралары

Бұл бөлімде СҮТ қызметінің КО-сында жүргізілетін физикалық, ұйымдастырушылық қорғау құралдарын және персоналдың әрекеттерін бақылау саласындағы негізгі іс-шаралар сипатталады.

24.1. Қауіпсіздікті қамтамасыз етудің физикалық шаралары

СҮТ қызметінің КО-сы бақыланатын аймақта – адамдардың және (немесе) көлік құралдарының болуы мен іс-әрекеттерін бақылау оның шегінде жүзеге асырылатын кеңістікте орналасады.

Комиссияда СҮТ қызметі КО-сының орналасуы мекенжайында орналасқан СҮТ қызметінің КО-сы пайдаланушыларының сертификаттарын алу үшін пайдаланылатын техникалық құралдар орналасқан үй-жайлардың қоршау конструкциялары, периметрлері СҮТ қызметінің КО-сы бақылайтын аймақтың физикалық шекарасы болып табылады.

24.2. Физикалық қол жетімділік

СҮТ қызметі КО-сының үй-жайлары Комиссияда орналасқан және қол жетімділікті бақылау және басқару жүйесімен жабдықталған. СҮТ қызметі КО-сының үй-жайына енуге авторланған персоналға ғана және СҮТ қызметі КО-сының жауапты қызметкерінің бірге жүруімен өзге де адамдарға рұқсат етіледі.

24.3. Электрмен жабдықтау және ауаны баптау

Негізгі қоректену жоғалған жағдайда жүйе автоматты түрде үздіксіз қоректендіру көздерінен резервтік қоректенуге көшеді.

СҮТ қызметі КО-сының серверлік үй-жайы ауаны баптау және желдету жүйесімен жарақтандырылған, ол микроклиматтың мынадай параметрлерін ұстап тұрады:

ауаның температурасы 18 – 24 °С шегінде (оның өзгеруінің шекті жылдамдығы – сағатына 3 °С);

ауаның ылғалдылығы ылғалдың конденсациясынсыз 30-дан 75 пайызға дейін (оның өзгеруінің шекті жылдамдығы – сағатына 6 пайыз);

шаңның шекті мөлшері - 10-6 г/м³ аспайды.

24.4. Ылғал әсеріне ұшырағыштығы

СҮТ қызметі КО-сының орналасқан жері су басудың табиғи қатерлеріне ұшырамайды.

24.5. Өртке қарсы қауіпсіздік шаралары және қорғау

СҮТ қызметі КО-сының серверлік үй-жайы МЕМСТ Р 53246-2008-ге және Ресей Федерациясы Үкіметінің 2012 жылғы 2 сәуірдегі № 390 қаулысымен бекітілген РФ-дағы өртке қарсы режим қағидаларына сәйкес автоматты өрт сөндіру жүйесімен жабдықталған.

24.6. Ақпарат жеткізгіштерді сақтау

СҮТ қызметінің КО-сында резервтік көшіру үшін USB жеткізгіштер пайдаланылады. Мұрағаттар сақталатын жеткізгіштер, сондай-ақ деректердің ағымдағы көшірмелері әкімшілік үй-жайларында орналасқан отқа төзімді сейфтерде сақталады.

24.7. Ақпарат жеткізгіштерді кәдеге жарату

Кілттік жеткізгіштер пайдалану құжаттамасына сәйкес форматталады және кілттерді сақтау үшін қайтадан пайдаланылады.

Аппараттық криптографиялық модульдер (HSM) өндірушінің пайдалану құжаттамасына сәйкес пайдалану аяқталғаннан кейін жойылады. HSM жою олар істен шыққан жағдайда сервис орталығына беру кезінде де жүргізіледі.

25. Персоналды басқару

25.1. Персоналдың біліктілігі

Қызмет көрсетуші персонал қолданысқа енгізілуі кезінде әзірленетін пайдалану құжаттамасында айқындалатын барлық қажетті рәсімдерді орындай алуға және:

ашық кілттер технологиясының негізгі ұғымдарын;

куәландырушы орталықтар қызметінің нормативтік-құқықтық негіздерін және заңдық жағынан маңызы бар электрондық құжат айналымын;

СҮТ қызметінің КО-сы бағдарламалық кешенінің тағайындалуын, негізгі сипаттамаларын және оның іске асырылатын алгоритмдерін;

СҮТ қызметінің КО-сы сервистерінің қызметін қамтамасыз ету кезінде құжаттармен жұмысты ұйымдастыру тәртібін;

дербес деректерді өңдеу тәртібін білуге тиіс.

25.2. Персоналға ұсынылатын құжаттама

СҮТ қызметі КО-сының басшылығы КО персоналына лауазымдық міндеттерді орындау үшін қажетті құжаттарға қол жетімділік береді.

26. Аудит журналдарын жүргізу

26.1. Тіркелетін оқиғалардың түрлері

СҮТ қызметі КО-сының БАК-ы оқиғалардың мынадай түрлерін:

жалпыжүйелік бағдарламалық қамтамасыз етудің жүйелі оқиғаларын;

сұрау салудың ЭЦҚ-ны тексеру сертификатына орналастырылуын;

сұрау салудың ЭЦҚ-ны тексеру сертификатына қабылдануын;

ЭЦҚ-ны тексеру кілті сертификатының шығарылуын;

ЭЦҚ-ны тексеру сертификатына сұрау салудың қабылданбауын;

кері қайтарылған ЭЦҚ-ны тексеру сертификаттарының шығарылуын;

бағдарламалық құрамдастың ішкі операциясының орындалмауын тіркейді.

Оқиғалар жазбаларының құрылымдары куәландырушы орталықтың нысаналы функцияларын іске асыруды бағдарламалық қамтамасыз етудің және жалпыжүйелік бағдарламалық қамтамасыз етудің пайдалану құжаттамасына сәйкес келеді.

26.2. Тіркелетін оқиғалардың жазбаларын өңдеу жиілігі

Тіркелетін оқиғалардың жазбаларын талдауды күн сайын аудит әкімшісі жүргізеді. Қауіпсіздік оқиғалары туындаған жағдайда тіркелетін оқиғалардың жазбаларын талдау осы оқиғаларды тергеп-тексеру шеңберінде жүргізіледі.

26.3. Тіркелетін оқиғалардың жазбаларын сақтау мерзімі

Тіркелетін оқиғалардың жазбалары жүйелі дискідегі файлдарда олар үшін берілген көлемнің ең көп мәнінен асуы сәтіне дейін сақталады. Осы уақыт кезеңінде олар уәкілетті тұлғаның немесе уәкілетті процестің сұрау салуы бойынша жедел режимде қол жетімді болады. Осы мерзім өткеннен кейін иеліктен шығарылатын жеткізгіштерде оқиғалар журналдарының резервтік көшірмесі жасалады.

Оқиғалар журналдарының резервтік көшірмелері белгіленген мерзім ішінде, кемінде 7 жыл сақталады.

26.4. Тіркелетін оқиғалардың жазбаларын қорғау

Оқиғалар журналдары қолданбалы және жалпыжүйелік бағдарламалық қамтамасыз ету құралдарымен қараудан, өзгертуден және жоюдан қорғалған.

26.5. Аудит жазбаларын жинау шарттары

Тіркелетін оқиғалар қолданбалы және жалпыжүйелік бағдарламалық қамтамасыз ету құралдарымен журналдарға автоматты түрде жазылады.

26.6. Тіркеу журналына енгізілген оқиға субъектісіне хабарлау

Тіркеу журналына оқиғаны жазу кезінде осы оқиғаның субъектісіне хабарлау жүргізілмейді.

27. Осалдықтарды талдау

Аудит әкімшісі пайдалану құжаттамасына сәйкес оқиғалар журналдарын мерзімдік қарау кезінде журналдардың мазмұнын КО бағдарламалық-техникалық құралдарына рұқсатсыз қол жеткізу (бұдан әрі – РҚЖ) әрекеттері туралы жазбалардың жоқтығы мәніне талдау жүргізеді. РҚЖ әрекеттері туралы жазбалар болған жағдайда осы факт туралы ақпараттық қауіпсіздік әкімшісіне хабарланады.

28. Мұрағатты жүргізу

28.1. Мұрағаттық жазбалардың түрлері

СҮТ қызметінің КО-сында деректердің мынадай түрлері:

алынатын өтінімдер, берілетін сертификаттар және түпкі пайдаланушыдан келіп түскен немесе оған файл немесе электрондық хабар нысанында берілген электрондық нысаны бар КСТ;

пайдаланушылардың тіркеу деректері;

берілген сертификаттардың тізілімі;

аудит журналдары;

СҮТ қызметі КО-сының пайдаланушылармен, сондай-ақ сенім білдіруші тараптармен ішкі және сыртқы хат-хабарлары (қағаз және электрондық нысандағы);

жеке басты куәландыру процесінде пайдаланылған құжаттар мен деректер мұрағаттауға жатады.

28.2. Мұрағатты сақтау мерзімі

СҮТ қызметінің КО-сы мұрағатты СҮТ қызметі КО-сының өнеркәсіптік пайдалануға іске қосылған сәтінен бастап оның қызметі тоқтатылған сәтке дейінгі КО-ны пайдаланудың бүкіл мерзімі бойында сақтайды.

28.3. Мұрағатты қорғау

СҮТ қызметі КО-сының мұрағаты бақыланатын аумақта орналастырылады. СҮТ қызметінің КО-сында сенім білдірілген рөлдерді орындайтын уәкілетті адамдар ғана мұрағатқа қол жетімділікті иеленеді.

28.4. Мұрағатты резервтік көшіру

Мұрағатталатын электрондық түрдегі барлық ақпарат сыртқы дербес жеткізгіштерге көшіріледі.

28.5. Мұрағаттың резервтік көшірмесіндегі деректерді қалпына келтіру

Резервтік көшірмедегі деректерді қалпына келтіруді пайдалану құжаттамасына сәйкес оператор орындайды. Резервтік көшірме деректерінің тұтастығын тексеру деректерді тікелей қалпына келтірудің алдында СҮТ қызметі КО-сының штаттық

бағдарламалық қамтамасыз ету құралдарымен автоматты түрде орындалады. Тұтастығы бұзылған жағдайда резервтік көшірмедегі деректерді қалпына келтіру орындалмайды.

29. СҮТ қызметінің КО-сы уәкілетті тұлғасының кілттерін және сертификатын ауыстыру

СҮТ қызметінің КО-сы уәкілетті тұлғасының кілті 3 жылда 1 реттен сиретпей ауыстырылады. Кілтті ауыстыру уәкілетті тұлғаның ЭЦҚ-ны тексеру кілтінің сертификатын ауыстырумен бірге жүргізіледі.

ЭЦҚ-ны тексеру кілттері сертификаттарының барлық иелері СҮТ қызметі КО-сының репозиторийінен СҮТ қызметінің КО-сы уәкілетті тұлғасының жаңа сертификатын алуға және оны алдыңғы сертификатты жоймастан СҮТС-ке орнатуға міндетті.

30. Компрометация және іркілістер кезіндегі қалпына келтіру

30.1. Компрометация жағдайында қалпына келтіру рәсімі

СҮТ қызметінің КО-сы уәкілетті тұлғасының ЭЦҚ кілтінің компрометациясы жағдайында СҮТ қызметінің КО-сы сертификаттарды қайтарып алудың кезектен тыс тізімін дайындайды, содан кейін СҮТ қызметінің КО-сы уәкілетті тұлғасының кілттері мен сертификатын ауыстыру жүргізіледі.

СҮТ қызметінің КО-сы компрометация фактісі туралы сертификаттардың иелерін және сенім білдіруші тараптарды хабардар ету бойынша мүмкін болатын барлық шараларды қабылдауға және ең қысқа мерзімде уәкілетті тұлғаның жаңа сертификатын пайдалана отырып барлық берілген сертификаттарды ауыстыруды жүргізуге міндетті.

30.2. Жабдықтардың бұзылу, бағдарламалық және (немесе) аппараттық іркіліс жағдайлары

Жабдықтардың бұзылу, бағдарламалық және (немесе) аппараттық іркіліс жағдайында оқиға туралы мәліметтерді Комиссияның осы фактіні анықтаған қызметкері СҮТ қызметі КО-сының басшысына және әкімшісіне хабарлайды, ол осы мәліметті басшылыққа жеткізеді, оқиғаны тергеп-тексереді және резервтік көшірмелер мен қосылқы жабдықты пайдалана отырып, салдарды жою бойынша қажетті шаралар қабылдайды.

30.3. СҮТ қызметі КО-сының ЭЦҚ кілтінің компрометациясы

Компрометациямен байланысты оқиғаларға мынадай оқиғалар жатады:

кілттік жеткізгіштерді жоғалту, оның ішінде олардың кейіннен табылуымен;

кілттік жеткізгіштерге немесе осы жеткізгіштердегі кілттік ақпаратқа қол жетімділігі бар қызметкерлердің кез келген себеп бойынша жұмыстан шығуы (осындай қол жетімділік мүмкіндігі жүйені ЭЦҚ құралдарымен нақты іске асыруға және осы жүйемен ақпаратты өңдеу технологиясына байланысты айқындалады);

жүйедегі ақпараттың жылыстауы немесе оның бұрмалануы туралы күдіктің туындауы;

кілттік жеткізгіштер бар сейфтегі мөр бүтіндігінің бұзылуы немесе осындай сейф кілтіне бақылауды жоғалту;

пайдаланушы жүйені пайдалану процесінде оның кілттік жеткізгішке қол жетімділікті шектеуге бақылауды жоғалтуы;

кілттік жеткізгішке не болғанын дәл анықтау мүмкін болмайтын жағдайлар (мысалы, оның бұзылуы және жеткізгішті бұзу қаскүнемнің оған қол жеткізу әрекетінің нәтижесінде болғандығы күдігін теріске шығарудың мүмкін болмауы);

нәтижесінде ЭЦҚ кілттері рұқсаты жоқ адамдарға және (немесе) процестерге қол жетімді болуы мүмкін кілттік ақпаратты жария етудің басқа да түрлері.

Санамаланған оқиғалар туындаған жағдайда СҮТ қызметінің КО-сында сенім білдірілген рөлді орындайтын ЭЦҚ кілтінің иесі ең қысқа мерзімде СҮТ қызметі КО-сының әкімшісіне хабарлайды және сертификатты кері қайтаруды сұратады. Жаңа сертификат алу осы Регламентте сипатталған тәртіппен жүзеге асырылады.

31. Авариядан кейін жұмыс қабілетін қалпына келтіру

СҮТ қызметі КО-сының персоналы деректердің резервтік көшірмелерін және қосалқы жабдықты пайдалана отырып, 8 сағаттан аспайтын уақыт ішінде КО-ның авариядан кейін жұмыс қабілетін қалпына келтіру бойынша мүмкін болатын барлық шараларды қабылдайды.

32. Техникалық қауіпсіздік шаралары

32.1. Кілттер жұбын генерациялау және орнату

32.1.1. Кілттер жұбын генерациялау

СҮТ қызметі КО-сының кілттер жұбы пайдалану құжаттамасына сәйкес әкімшінің автоматтандырылған жұмыс орнында (АЖО) жасалады. КО кілттерін генерациялауды сертификаттау әкімшісі СҮТ қызметі КО-сының ақпараттық қауіпсіздік әкімшісімен бірлесіп жүзеге асырады.

СҮТ қызметі КО-сының СМТС пен УШС кілттерінің жұптары пайдалану құжаттамасына сәйкес КО серверінде жасалады. КО кілттерін генерациялауды СҮТ қызметі КО-сының сертификаттау әкімшісі жүзеге асырады.

Интеграциялық жүйенің ұлттық сегменттерінің және интеграциялық сегментінің СҮТ ТРС және УШС кілттерінің жұптарын СҮТ кіші жүйесіне арналған пайдалану құжаттамасына сәйкес тікелей СҮТ серверінде СҮТ операторының уәкілетті қызметкері жасайды.

Комиссияның КО мен СҮТ-тегі кілттерін генерациялау үшін ЭЦҚ құралдарының сенім білдірілген есептеу құрылғысы (ЭЦҚ СЕҚ) пайдаланылады. Сақталатын кілттік

ақпаратты қорғау үшін арнайы дайындалған USB-flash жеткізгіштері қосымша пайдаланылады.

СЕҚ-тағы ЭЦҚ кілтін инициализациялау үшін СЕҚ-та сақталатын ақпараттың болуынан басқа, қол жеткізу паролін енгізу және USB-flash жеткізгіште сақталатын деректер қосымша талап етіледі.

32.1.1.1. Пайдаланушыға ЭЦҚ-ның жеке кілтін ұсыну

СҮТ қызметі КО-сының пайдаланушылардың ЭЦҚ кілттеріне қол жетімділігі жоқ, өйткені осы Регламентке сәйкес әрбір пайдаланушы кілттер жұбын генерациялауды дербес жүзеге асырады.

32.1.1.2. СҮТ қызметінің КО-сына ЭЦҚ-ны тексеру кілтін беру

Пайдаланушы кілттерді өз бетімен генерациялауды жүзеге асырады және электрондық жеткізгіштерді пайдалана отырып, электрондық түрдегі сертификатқа сұрау салу файлының құрамында ЭЦҚ-ны тексеру кілтін СҮТ қызметінің КО-сына береді.

32.1.1.3. ЭЦҚ-ны тексеру кілтін сенім білдіруші тараптарға ұсыну

СҮТ қызметі КО-сының ЭЦҚ-ны тексеру кілтін сенім білдіруші тараптарға беру ЭЦҚ-ны тексеру кілтін қамтитын ЭЦҚ-ны тексеру кілтінің сертификатын СҮТ қызметі КО-сының репозиторийінде жариялау жолымен жүзеге асырылады.

СҮТ қызметінің КО-сы берген барлық сертификаттар СҮТ қызметі КО-сының репозиторийінде жарияланған СҮТ қызметі КО-сының түбір сертификатының файлына сілтемесі бар AuthorityInformationAccess кеңейтуді қамтиды.

32.1.2. Кілттердің мөлшерлері

ЭЦҚ-ның пайдаланылатын құралдарына арналған пайдалану құжаттамасына сәйкес кілттердің мөлшерлері мыналарды құрайды:

электрондық цифрлық қолтаңба кілттерінің ұзындығы:

электрондық цифрлық қолтаңба кілті – 512 бит;

электрондық цифрлық қолтаңбаны тексеру кілті – 1024 бит;

шифрлау кезінде пайдаланылатын кілттердің ұзындығы:

симметриялық кілт – 256 бит.

32.1.3. ЭЦҚ-ны тексеру кілтін генерациялау параметрлері және кілттердің сапасын тексеру

СҮТ қызметінің КО-сын пайдаланушылар кілттерді генерациялау үшін СЕҚ-ты пайдаланады. Бұл ретте СЕҚ құрамындағы SSD-диск кілттік жеткізуші болып табылады. Кілттік жеткізушілер ретінде кілттік жеке USB-жеткізгіштері де пайдаланылады.

ЭЦҚ-ны тексеру кілтін генерациялау параметрлерін пайдаланылатын ЭЦҚ құралы автоматты түрде береді.

Кілттерді генерациялау алгоритмі ЕЭК Алқасының 2.06.16 ж. № 49 ҚБПҮ шешіміне сай МЕМСТ Р 34.10-2012-ге сәйкес келеді.

Сертификатқа сұрау салуды алу кезінде СҮТ қызметінің КО-сы сұрау салуда алынған кілттің пайдаланылатын ЭЦҚ құралына үйлесімділігін, оның разрядтылығын, сондай-ақ оның бірегейлігін тексереді. Алынған кілт СҮТ қызметі КО-сының дерекқорында бар кілтке сәйкес келген жағдайда СҮТ қызметінің КО-сы сұрау салуды қабылдамайды және қайталама кілтпен сұрау салу берген пайдаланушыға жаңа кілттер жұбы мен сертификатқа сұрау салуды генерациялау қажеттігі туралы хабарлайды.

32.1.4. Кілттерді пайдалану мақсаттары

Кілтті қолдану тәсілі X.509 v3 сәйкес келетін сертификаттың стандарттық кеңейтулерінің KeyUsage жолағында айқындалған.

СҮТ қызметінің КО-сы уәкілетті тұлғасының кілті шығарылатын сертификаттарда (бит 5 keyCertSign) және КСТ-да (бит 6 cRLSign) ЭЦҚ қалыптастыру үшін ғана пайдаланылуы мүмкін.

Түпкі пайдаланушылардың кілттері ЭЦҚ қалыптастыру үшін пайдаланылады. KeyUsage жолағындағы әрбір битті пайдалану RFC 5280-де жазылған қағидаларға сәйкес келеді.

32.1.5. СҮТ қызметінің КО-сы уәкілетті тұлғасының ЭЦҚ кілтін қорғау

СҮТ қызметінің КО-сы уәкілетті тұлғасының (сертификаттау әкімшісінің) ЭЦҚ кілті СҮТ қызметінің КО-сы әкімшісінің АЖО ЭЦҚ СЕҚ-ында қорғалған (шифрланған) түрде сақталады.

СЕҚ-та уәкілетті тұлғаның ЭЦҚ кілтін инициализациялау үшін КО әкімшілерінің кілттік жеткізгіштерін дәйекті түрде енгізу (ену парольдерін енгізе отырып) және СЕҚ құрамындағы SSD-дискіде сақталатын қызметтік деректердің болуы талап етіледі.

Уәкілетті тұлғаның ЭЦҚ кілті пайдаланылу кезеңінде (жасалған сәтінен бастап жойылған сәтіне дейін) ЭЦҚ СЕҚ-ында болады және қандай да бір сыртқы жеткізгіштерге иеліктен шығарылмайды (ЭЦҚ СЕҚ кілттерін депозиттеу функциясы сақталмайды).

32.1.6. Криптографиялық модульдің стандарттары

Кілттердің форматтары мен аппараттық криптографиялық модульмен орындалатын криптографиялық операциялар МЕМСТ Р 34.10-2012 және МЕМСТ Р 34.11-2012 стандарттарына сәйкес келеді.

32.1.7. ЭЦҚ кілттерін депозиттеу

СҮТ қызметінің КО-сы ЭЦҚ кілттерін депозиттеуді жүзеге асырмайды.

32.1.8. ЭЦҚ кілтінің резервтік көшірмесі

СҮТ қызметінің КО-сы ЭЦҚ кілттерін резервтеуді жүзеге асырмайды.

32.1.9. Қолданылу мерзімі аяқталғаннан кейін ЭЦҚ кілтін сақтау

ЭЦҚ кілті қолданылу мерзімі аяқталғаннан кейін ЭЦҚ құралдарының және СҮТ қызметінің КО-сы құралдарының штаттық функциялары пайдаланыла отырып жойылуға жатады.

32.1.10. СҮТ қызметі КО-сының ЭЦҚ кілтін жасау және жою

СҮТ қызметінің КО-сы уәкілетті тұлғасының ЭЦҚ кілті жасалған сәттен бастап пайдаланудан шығару кезінде жойылғанға дейін СЕҚ-та тұрақты түрде болады.

32.1.11. ЭЦҚ кілтін криптографиялық модульде сақтау

СҮТ қызметінің КО-сы уәкілетті тұлғасының ЭЦҚ кілті аппараттық криптографиялық модульде шифрланған түрде сақталады.

32.1.12. ЭЦҚ кілтін активтендіру тәсілі

СҮТ қызметінің КО-сы уәкілетті тұлғасының ЭЦҚ кілті КО әкімшілерінің алмалы-салмалы кілттік жеткізгіштерінің дәйекті ұсынылуы (қол жеткізу парольдерін енгізе отырып) және СЕҚ құрамындағы SSD-дискіде сақталатын қызметтік деректердің болуы кезінде инициализацияланады.

32.1.13. Репозиторийді резервтік көшіру

СҮТ қызметі КО-сының репозиторийі СҮТ қызметінің КО-сында белгіленген резервтік көшіру тәртібіне сәйкес мерзімдік резервтік көшіруге жатады.

32.1.14. Сертификаттар мен кілттердің қолданылу мерзімдері

ЭЦҚ кілттерінің және ЭЦҚ-ны тексеру кілттері сертификаттарының қолданылу мерзімдері пайдаланылатын ЭЦҚ құралының пайдалану құжаттамасымен айқындалады
.

СҮТ қызметі КО-сының кілттері мен сертификаттарының қолданылу мерзімдері:

ЭЦҚ кілттері қолданысының ең ұзақ мерзімі – 3 жылға дейін;

ЭЦҚ-ны тексеру кілттері қолданысының ең ұзақ мерзімі – 7 жылға дейін.

Пайдаланушылардың кілттері мен сертификаттарының қолданылу мерзімдері:

ЭЦҚ кілттері қолданысының ең ұзақ мерзімі – 3 жылға дейін;

ЭЦҚ-ны тексеру кілттері қолданысының ең ұзақ мерзімі – 7 жылға дейін.

32.1.15. Активтендіру деректері

СҮТ қызметі КО-сының ЭЦҚ кілттері үшін активтендіру деректері ретінде мыналар әрекет етеді:

СҮТ USB-flash жеткізгіштен оқитын деректер;

USB-flash жеткізгішке қол жеткізу парольдері;

СЭҚ-тың SSD-дискісінде сақталатын қызметтік деректер.

33. Бағдарламалық-аппараттық қамтамасыз етудің қауіпсіздігі

СҮТ қызметі КО-сының бағдарламалық-аппараттық кешенінің қауіпсіздігін қамтамасыз ету жөніндегі іс-шараларды СҮТ қызметі КО-сының ақпараттық қауіпсіздік әкімшісі жүзеге асырады.

АЖО-ға және КО серверлеріне бағдарламалық қамтамасыз етуді және оны теңшеуді СҮТ қызметі КО-сының жүйелік әкімшісі эталондық дискіден жүзеге асырады.

Серверлердің корпусы, әкімшінің АЖО-сы және СЕҚ пайдалану құжаттамасына сәйкес СҮТ қызметі КО-сының ақпараттық қауіпсіздік әкімшісінің жеке мөрімен мөрленеді. Жұмыс басталар алдында корпустың және мөрлердің (пломбалардың)

бүтіндігіне визуалдық бақылау жасалады. Корпустың ашылғаны және/немесе мөрлердің (пломбалардың) бүлінгені анықталған жағдайда одан арғы жұмысқа тыйым салынады, осы факт туралы КО басшылығына баяндалады.

КО техникалық құралдарын пайдалану процесінде СҮТ қызметі КО-сының құрамына, конструкциясына, электр және монтаждау схемаларына өзгеріс енгізуге тыйым салынады.

Техникалық құралдарды жөндеу көрсетілген құралдарды дайындаған кәсіпорында жүзеге асырылады. Жөндеу жүргізілгеннен кейін техникалық құралдарды арнайы тексеру және арнайы зерттеу жүргізіледі.

КО құрамына қосымша аппарат құралдарын енгізуге тақырыптық зерттеулер, арнайы тексерулер және осы құралдарға арнайы зерттеулер жүргізбей жол берілмейді.

34. Жұмыс істеу ортасының тұтастығын бақылау құралдары

КО құралдарын бағдарламалық қамтамасыз етудің және жұмыс істеу ортасының тұтастығын динамикалық бақылау құралдары QP ОС базалық операциялық жүйесінің құрамына кіреді.

Тұтастықты бастапқы және кезеңдік бақылау СҮТ қызметі КО-сының ТҚ құрамындағы СЖАБМ құралдарымен орындалады.

35. Желілік қауіпсіздік

Желілік қауіпсіздік трафикті сүзу арқылы желіаралық экрандардың көмегімен, сондай-ақ желіні сегменттеумен қамтамасыз етіледі. Желіаралық экрандарда жүйенің кідіріссіз жұмыс істеуі үшін қажетті порттар мен хаттамалар бойынша қосуға рұқсат етілген. Қалған барлық порттар мен хаттамаларға қол жетімділік жоқ. Жалпыға бірдей қол жетімді деректерді жариялау үшін желінің жеке сегменті бөлінген.

Сыртқы сегментте рұқсатсыз енуді анықтау құралы пайдаланылады.

Еуразиялық экономикалық
одақтың интеграцияланған
ақпараттық жүйесінің сенім
білдірілген үшінші тарапы
қызметі куәландырушы
орталығының регламентіне
№ 1 ҚОСЫМША

Сертификаттарға сұрау салулардың, сертификаттардың және кері қайтарылған сертификаттар тізімдерінің ШАБЛОНДАРЫ

Сертификатқа сұрау салу шаблоны

Сертификатқа сұрау салу PKCS#10 форматындағы құрылымды білдіреді және үш жолақтың дәйектілігі болып табылады, олардың біріншісі сұрау салудың негізгі сұлбасын (certificationRequestInfo), екіншісі – сертификатқа сұрау салуға қол қою үшін

пайдаланылған алгоритмнің тұрпаты туралы ақпаратты (signatureAlgorithm), ал үшіншісі – сұрау салуға қол қойған электрондық цифрлық қолтаңбаны (signatureValue) қамтиды.

СҮТ қызметі КО-сының ЭЦҚ сертификаттарына сұрау салулар кем дегенде мынадай негізгі жолақтарды қамтиды:

Version: сертификатқа сұрау салу форматының бірінші нұсқасы (v1(0));

Subject: сертификат алатын түпкі пайдаланушының бірегей атауы (DN);

SubjectPublicKeyInfo: алгоритм сәйкестендіргішімен бірге ашық кілттің мәні;

Attributes: сертификатта сақталатын кеңейтулер туралы ақпаратты қамтуы мүмкін атрибуттардың коллекциясы.

Негізгі жолақтар мен кеңейтулердің мәндері ЭЦҚ-ны тексеру кілтінің сертификаты оған сәйкес берілетін саясатқа байланысты айқындалады.

СҮТС серверінің сертификатына сұрау салу

Жолақтың атауы	**мән немесе мәнді шектеулер**
Version (нұсқа)	Version 1
Subject (субъект, DN атауы)	DN атауы X.501 талаптарына сәйкес келеді. Common Name (CN) = <СҮТ сервисінің атауы>, Organization (O) = <Ұйымның қысқартылған атауы>, Organization Unit (OU) = <Бөлімшенің атауы>, mailAddress (E) = <СҮТ БАК әкімшісі электрондық поштасының мекенжайы>
Subject Public Key Info (субъектінің ашық кілті)	кодталатын жолақ RFC 2986-да сипатталған талаптарға сәйкес келеді және ашық кілттер туралы МЕМСТ 34.10-2012 ақпаратты қамтиды (яғни кілттің сәйкестендіргіші мен биттардағы кілттің ұзындығымен және ашық кілттің мәндері).
KeyUsage (OID кеңейту 2.5.29.15) (кілтті пайдалану) – Attributes-те қамтылады	digitalSignature, nonRepudiation
ExtendedKeyUsage (OID кеңейту 2.5.29.37) (кілтті кеңейтілген пайдалану) – Attributeste қамтылады	Dvcs (OID 1.3.6.1.5.5.7.3.10)
SubjectKeyIdentifier (OID кеңейту 2.5.29.14) – Attributeste қамтылады	субъектінің ашық кілтінің бірегей сәйкестендіргіші
CertificatePolicy (OID кеңейту 2.5.29.32) (сертификат саясаты) – Attributeste қамтылады	саясат сәйкестендіргіші: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id-_____(X) …
Signature Algorithm (қолтаңба алгоритмі)	МЕМСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Signature (қолтаңба)	сертификатқа сұрау салудың қолтаңбасы RFC 2986-да айқындалған талаптарға сәйкес генерацияланады және кодталады.

СМТС серверінің сертификатына сұрау салу

Жолақтың атауы	**Мән немесе мәнді шектеулер**

Version (нұсқа)	Version 1
Signature Algorithm (қолтаңба алгоритмі)	МЕМСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Subject (субъект, DN атауы)	DN атауы X.501 талаптарына сәйкес келеді. Common Name (CN) = <Псевдоним СПСС>, Organization (O) = <Ұйымның қысқартылған атауы>, Organization Unit (OU) = <Бөлімшенің атауы>, mailAddress (E) = <OCSP сервер әкімшісінің электрондық поштасының мекенжайы>
Subject Public Key Info (субъектінің ашық кілті)	кодталатын жолақ RFC 2986-да сипатталған талаптарға сәйкес келеді және ашық кілттер туралы МЕМСТ 34.10-2012 ақпаратты қамтиды (яғни кілттің сәйкестендіргіші мен биттардағы кілттің ұзындығымен және ашық кілттің мәндері).
KeyUsage (OID кеңейту 2.5.29.15) (кілтті пайдалану) – Attributeste қамтылады	digitalSignature, nonRepudiation,
ExtendedKeyUsage (OID кеңейту 2.5.29.37) (кілтті кеңейтілген пайдалану) – Attributeste қамтылады	OCSPSigning (OID 1.3.6.1.5.5.7.3.9)
SubjectKeyIdentifier (OID кеңейту 2.5.29.14) – Attributeste қамтылады	субъектінің ашық кілтінің бірегей сәйкестендіргіші
CertificatePolicy (OID кеңейту 2.5.29.32) (сертификат саясаты) – Attributeste қамтылады	саясат сәйкестендіргіші: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id-_____(X) …
Signature Algorithm (қолтаңба алгоритмі)	МЕМСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Signature (қолтаңба)	сертификаттың қолтаңбасы RFC 2986-да айқындалған талаптарға сәйкес генерацияланады және кодталады.

УШС серверінің сертификатына сұрау салу

Жолақтың атауы	**Мән немесе мәнді шектеулер**
Version (нұсқа)	Version 1
Subject (субъект, DN атауы)	DN атауы X.501 талаптарына сәйкес келеді. Common Name (CN) = <Псевдоним СШВ>, Organization (O) = <Ұйымның қысқартылған атауы>, Organization Unit (OU) = <Бөлімшенің атауы>, mailAddress (E) = <адрес электронной почты администратора TSP сервер әкімшісінің электрондық поштасының мекенжайы>
Subject Public Key Info (субъектінің ашық кілті)	кодталатын жолақ RFC 2986-да сипатталған талаптарға сәйкес келеді және ашық кілттер туралы МЕМСТ 34.10-2012 ақпаратты қамтиды (яғни кілттің сәйкестендіргіші мен биттардағы кілттің ұзындығымен және ашық кілттің мәндері).
KeyUsage (OID кеңейту 2.5.29.15) (кілтті пайдалану) – Attributeste қамтылады	digitalSignature, nonRepudiation,

ExtendedKeyUsage (OID кеңейту 2.5.29.37) (кілтті кеңейтілген пайдалану) – Attributeste қамтылады	timestamping (OID 1.3.6.1.5.5.7.3.8)
SubjectKeyIdentifier (OID кеңейту 2.5.29.14) – Attributeste қамтылады	субъектінің ашық кілтінің бірегей сәйкестендіргіші
CertificatePolicy (OID кеңейту 2.5.29.32) (сертификат саясаты) – Attributeste қамтылады	саясат сәйкестендіргіші: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id-_____(X) …
Signature Algorithm (қолтаңба алгоритмі)	МЕМСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Signature (қолтаңба)	сертификаттың қолтаңбасы RFC 2986-да айқындалған талаптарға сәйкес генерацияланады және кодталады

ЭЦҚ-ны тексеру кілті сертификатының шаблоны

ЭЦҚ-ны тексеру кілтінің сертификаты X.509 v.3 стандартына сәйкес үш жолақтың дәйектілігі болып табылады, олардың біріншісі сертификаттың ішіндегісін (tbsCertificate)), екіншісі – сертификатқа қол қою үшін пайдаланылған алгоритмнің тұрпаты туралы ақпаратты (signatureAlgorithm), ал үшіншісі – сертификатқа қол қойған электрондық цифрлық қолтаңбаны (signatureValue) қамтиды.

СҮТ қызметі КО-сының ЭЦҚ-ны тексеру кілттерінің сертификаттары кем дегенде мынадай негізгі жолақтарды қамтиды:

Version: сертификат форматының үшінші нұсқасы (X.509 v.3);

SerialNumber: куәландырушы орталықтың шеңберінде бірегей сертификаттың сериялық нөмірі;

Signature Algorithm: сертификатқа қол қою үшін сертификаттар беретін куәландырушы орталық қолданатын алгоритмнің сәйкестендіргіші;

Issuer: Куәландырушы орталықтың бірегей атауы (DN);

Validity: сертификат қолданысының басталуын (notBefore) және аяқталуын (notAfter) айқындайтын сертификаттың қолданылу мерзімі;

Subject: сертификат алатын түпкі пайдаланушының бірегей атауы (DN);

SubjectPublicKeyInfo: алгоритм сәйкестендіргішімен бірге ашық кілттің мәні;

Signature: қолтаңба RFC 5280 сәйкес генерацияланады және кодталады.

Негізгі жолақтар мен кеңейтулердің мәндері ЭЦҚ-ны тексеру кілтінің сертификаты оған сәйкес берілетін саясатқа байланысты айқындалады.

СҮТС серверінің сертификаты

Жолақтың атауы	**мән немесе мәнді шектеулер**
Version (нұсқа)	Version 3
Serial Number (сериялық нөмірі)	СҮТ қызметінің КО беретін барлық сертификаттардағы бірегей мән
Signature Algorithm (қолтаңба алгоритмі)	МЕМСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
	Common Name (CN) = СҮТ қызметінің КО-сы,

Issuer (баспагер, DN атауы)	Organization (O) = ЕЭК, Organization Unit (OU) = ИТ, Country (C) = RU
Not before (қолданылу мерзімінің басы)	UTC (Universal Coordinate Time) сәйкес негізгі уақыт
Not after (қолданылу мерзімінің аяғы)	UTC (Universal Coordinate Time) сәйкес негізгі уақыт
Subject (субъект, DN атауы)	DN атауы X.501 талаптарына сәйкес келеді. Common Name (CN) = <СҮТ сервисінің атауы>, Organization (O) = <Ұйымның қысқартылған атауы>, Organization Unit (OU) = <Бөлімшенің атауы>, mailAddress (E) = <СҮТ БАК әкімшісінің электрондық поштасының мекенжайы>
Subject Public Key Info (субъектінің ашық кілті)	кодталатын жолақ RFC 2986-да сипатталған талаптарға сәйкес келеді және ашық кілттер туралы МЕМСТ 34.10-2012 ақпаратты қамтиды (яғни кілттің сәйкестендіргіші мен биттардағы кілттің ұзындығымен және ашық кілттің мәндері).
KeyUsage (OID кеңейту 2.5.29.15) (кілтті пайдалану)	digitalSignature, nonRepudiation
ExtendedKeyUsage (OID кеңейту 2.5.29.37) (кілтті кеңейтілген пайдалану)	Dvcs (OID 1.3.6.1.5.5.7.3.10)
CertificatePolicy (OID кеңейту 2.5.29.32) (сертификат саясаты)	саясат сәйкестендіргіші: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id-_____(X) …
AuthorityInformationAccess (OID кеңейту 1.3.6.1.5.5.7.1.1) (СҮТ қызметі КО УЛ сертификатына қол жетімділік)	СҮТ қызметі КО УЛ сертификаты файлының мынадай түрдегі URL: http:// <XXX>00.DTS.EEC/RootTTPCA.crt, http:// <XXX>01.DTS.EEC/RootTTPCA.crt СМТС серверінің мынадай түрдегі URL: http:// <XXX>00.DTS.EEC/<псевдоним_СМТС>/ ocsp.srf, http:// <XXX>01.DTS.EEC/< псевдоним_СМТС>/ocsp.srf
CRLDistributionPoint (OID кеңейту 2.5.29.31) (КСТ қолданылу нүктесі)	СҮТ қызметі КО КСТ файлының URL: http:// <XXX>00.DTS.EEC/RootTTPCA.crl, http:// <XXX>01.DTS.EEC/RootTTPCA.crl
BasicConstraints (OID кеңейту 2.5.29.19)	түпкі субъект
SubjectKeyIdentifier (OID кеңейту 2.5.29.14)	субъектінің ашық кілтінің бірегей сәйкестендіргіші
Signature (қолтаңба)	сертификаттың қолтаңбасы RFC 5280-де айқындалған талаптарға сәйкес генерацияланады және кодталады

СМТС серверінің сертификаты

Жолақтың атауы	**мән немесе мәнді шектеулер**

Version (нұсқа)	Version 3
Serial Number (сериялық нөмірі)	СҮТ қызметінің КО беретін барлық сертификаттардағы бірегей мән
Signature Algorithm (қолтаңба алгоритмі)	МЕМСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (баспагер, DN атауы)	Common Name (CN) = СҮТ қызметінің КО-сы, Organization (O) = ЕЭК, Organization Unit (OU) = ИТ, Country (C) = RU
Not before (қолданылу мерзімінің басы)	UTC (Universal Coordinate Time) сәйкес негізгі уақыт
Not after (қолданылу мерзімінің аяғы)	UTC (Universal Coordinate Time) сәйкес негізгі уақыт
Subject (субъект, DN атауы)	DN атауы X.501 талаптарына сәйкес келеді. Common Name (CN) = <Псевдоним СМТС>, Organization (O) = <Ұйымның қысқартылған атауы>, Organization Unit (OU) = <Бөлімшенің атауы>, mailAddress (E) = <OCSP сервер әкімшісінің электрондық поштасының мекенжайы>
Subject Public Key Info (субъектінің ашық кілті)	кодталатын жолақ RFC 2986-да сипатталған талаптарға сәйкес келеді және ашық кілттер туралы МЕМСТ 34.10-2012 ақпаратты қамтиды (яғни кілттің сәйкестендіргіші мен биттардағы кілттің ұзындығымен және ашық кілттің мәндері).
KeyUsage (OID кеңейту 2.5.29.15) (кілтті пайдалану)	digitalSignature, nonRepudiation,
ExtendedKeyUsage (OID кеңейту 2.5.29.37) (кілтті кеңейтілген пайдалану)	OCSPSigning (OID 1.3.6.1.5.5.7.3.9)
CertificatePolicy (OID кеңейту 2.5.29.32) (сертификат саясаты)	саясат сәйкестендіргіші: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id-_____(X) …
AuthorityInformationAccess (OID кеңейту 1.3.6.1.5.5.7.1.1) (СҮТ қызметі КО УЛ сертификатына қол жетімділік)	СҮТ қызметі КО УЛ сертификаты файлының мынадай түрдегі URL: http:// <XXX>00.DTS.EEC/RootTTPCA.crt, http:// <XXX>01.DTS.EEC/RootTTPCA.crt СМТС серверінің мынадай түрдегі URL: http:// <XXX>00.DTS.EEC/<псевдоним_СМТС>/ ocsp.srf, http:// <XXX> 01.DTS.EEC/< псевдоним_СМТС>/ocsp.srf
SubjectKeyIdentifier (OID 2.5.29.14)	субъектінің ашық кілтінің бірегей сәйкестендіргіші
CRLDistributionPoint (OID кеңейту 2.5.29.31) (КСТ қолданылу нүктесі)	СҮТ қызметі КО КСТ файлының URL: http:// <XXX>00.DTS.EEC/RootTTPCA.crl, http:// <XXX>01.DTS.EEC/RootTTPCA.crl

Signature (қолтаңба)	сертификаттың қолтаңбасы RFC 5280-де айқындалған талаптарға сәйкес генерацияланады және кодталады

УШС серверінің сертификаты

Жолақтың атауы	**мән немесе мәнді шектеулер**
Version (нұсқа)	Version 3
Serial Number (сериялық нөмірі)	СҮТ қызметінің КО беретін барлық сертификаттардағы бірегей мән
Signature Algorithm (қолтаңба алгоритмі)	МЕМСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (баспагер, DN атауы)	Common Name (CN) = СҮТ қызметінің КО-сы, Organization (O) = ЕЭК, Organization Unit (OU) = ИТ, Country (C) = RU
Not before (қолданылу мерзімінің басы)	UTC (Universal Coordinate Time) сәйкес негізгі уақыт
Not after (қолданылу мерзімінің аяғы)	UTC (Universal Coordinate Time) сәйкес негізгі уақыт
Subject (субъект, DN атауы)	DN атауы X.501 талаптарына сәйкес келеді. Common Name (CN) = <Псевдоним СШВ>, Organization (O) = <Ұйымның қысқартылған атауы>, Organization Unit (OU) = <Бөлімшенің атауы>, mailAddress (E) = <TSP сервер әкімшісінің электрондық поштасының мекенжайы >
Subject Public Key Info (субъектінің ашық кілті)	кодталатын жолақ RFC 2986-да сипатталған талаптарға сәйкес келеді және ашық кілттер туралы МЕМСТ 34.10-2012 ақпаратты қамтиды (яғни кілттің сәйкестендіргіші мен биттардағы кілттің ұзындығымен және ашық кілттің мәндері).
KeyUsage (OID кеңейту 2.5.29.15) (кілтті пайдалану)	digitalSignature, nonRepudiation
ExtendedKeyUsage (OID кеңейту 2.5.29.37) (кілтті кеңейтілген пайдалану)	timestamping (OID 1.3.6.1.5.5.7.3.8)
CertificatePolicy (OID кеңейту 2.5.29.32) (сертификат саясаты)	саясат сәйкестендіргіші: iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id-_____(X) …
SubjectKeyIdentifier (OID кеңейту 2.5.29.14)	субъектінің ашық кілтінің бірегей сәйкестендіргіші
AuthorityInformationAccess (OID кеңейту 1.3.6.1.5.5.7.1.1) (СҮТ қызметі КО УЛ сертификатына қол жетімділік)	СҮТ қызметі КО УЛ сертификаты файлының мынадай түрдегі URL: http:/ <XXX>00.DTS.EEC/RootTTPCA.crt, http:// <XXX>01.DTS.EEC/RootTTPCA.crt СМТС серверінің мынадай түрдегі URL: http://<XXX>00.DTS.EEC/<псевдоним_СМТС>/ ocsp.srf, http://<XXX>01.DTS.EEC/< псевдоним_СМТС>/ocsp.srf

CRLDistributionPoint (OID кеңейту 2.5.29.31) (КСТ қолданылу нүктесі)	СҮТ қызметі КО КСТ файлының URL: http:// <XXX>00.DTS.EEC/RootTTPCA.crl, http:// <XXX>01.DTS.EEC/RootTTPCA.crl
Signature (қолтаңба)	сертификаттың қолтаңбасы RFC 5280-де айқындалған талаптарға сәйкес генерацияланады және кодталады

Нұсқа нөмірі

ЭЦҚ-ны тексеру кілттерінің барлық сертификаттарын X.509 v.3 нұсқасына сәйкес СҮТ қызметінің КО-сы береді.

ЭЦҚ-ны тексеру кілті сертификатын кеңейту

Әрбір кеңейтудің функциясы онымен байланысты объект сәйкестендіргішінің (OBJECT IDENTIFIER) стандарттық мәнімен айқындалады. ЭЦҚ-ны тексеру кілтінің сертификатын беретін СҮТ қызметінің КО-сы таңдап алған опцияға байланысты кеңейту сыни немесе сыни емес болуы мүмкін. Егер кеңейту сыни ретінде белгіленсе, онда ЭЦҚ-ны тексеру кілттерінің сертификаттарын пайдаланатын қосымша ЭЦҚ-ны тексеру кілтінің әрбір сертификатын қабылдамауға тиіс, ондағы сыни кеңейту анықталғаннан кейін ол оны айырып тани алмайды. Әрбір сыни емес кеңейтудің ескерілмеуі мүмкін.

Кілтті пайдалану (Key Usage)

Кілтті пайдалануды шешу – сыни немесе сыни емес болуы мүмкін. Осы кеңейту кілтті қолдану тәсілін айқындайды (мысалы деректерді шифрлауға арналған кілт, ЭЦҚ арналған кілт және т.б.). Осы кеңейтудің мәні ЭЦҚ-ны тексеру кілтінің сертификаты оған сәйкес берілген саясатқа байланысты.

СҮТС серверінің сертификаты

СҮТ серверінің сертификатындағы "Кілтті пайдалану" деген кеңейту сыни ретінде белгіленеді және оның мынадай мәндері бар:

digitalSignature (0) – цифрлық қолтаңбаны іске асыруға (субъектіні немесе деректерді сәйкестендіруге) арналған кілт;

nonRepudiation (1) – бас тартпаушылықты іске асырумен байланысты кілт;

ЭЦҚ-ны тексеру кілті сертификатының мәртебесін тексеру сервисінің сертификаты

СМТС сертификатында "Кілтті пайдалану" деген кеңейту сыни ретінде белгіленеді және оның мынадай мәндері бар:

digitalSignature (0) – цифрлық қолтаңбаны іске асыруға (субъектіні немесе деректерді сәйкестендіруге) арналған кілт;

nonRepudiation (1) – бас тартпаушылықты іске асырумен байланысты кілт;

Уақыт штамптары сервисінің сертификаты

УШС сертификатында "Кілтті пайдалану" деген кеңейту сыни ретінде белгіленеді және оның мынадай мәндері бар:

digitalSignature (0) – цифрлық қолтаңбаны іске асыруға (субъектіні немесе деректерді сәйкестендіруге) арналған кілт;

nonRepudiation (1) – бас тартпаушылықты іске асырумен байланысты кілт;

Жақсартылған кілт (ExtendedKeyUsage)

Кілтті пайдалануды нақтылау (шектеу) – кеңейту сыни болуы мүмкін. Бұл жолақ шегінде сертификат пайдаланылуы мүмкін keyUsage жолағында белгіленген негізгі қолдануға қосымша ретінде бір немесе одан да көп салаларды айқындайды. Бұл жолақты keyUsage жолағында айқындалған кілтті қолданудың жол берілетін саласын шектеу ретінде түсіндіру қажет. Кеңейтудің нақты мәндері ЭЦҚ-ны тексеру кілтінің сертификаты оған сәйкес берілген саясатқа байланысты болады.

Сертификаттың мәртебесін тексеру сервисінің сертификаты

СМТС сертификатында кеңейту сыни емес ретінде белгіленеді және OCSPSigning объектілік сәйкестендіргішін қамтиды: 1.3.6.1.5.5.7.3.9.

Уақыт штамптары сервисінің сертификаты

УШС сертификатында кеңейту сыни емес ретінде белгіленеді және Timestaping объектілік сәйкестендіргішін қамтиды: 1.3.6.1.5.5.7.3.8.

Сертификат саясаттары (Certificate Policy)

Сертификаттарды қолдану саясатын кеңейту (CertificatePolicies) СҮТ қызметі КО-сының Регламентінде сипатталған қағидаларға сәйкес ЭЦҚ-ны тексеру кілтінің сертификатына енгізілетін саясаттарды сәйкестендіргіштер мен оның квалификаторларын қамтиды. Бұл кеңейту сыни кеңейту болып табылмайды.

Негізгі шектеулер (Basic Constraints)

Куәландырушы орталықтардың ЭЦҚ-ны тексеру кілттерінің сертификаттарындағы кеңейту сыни болып табылады және түпкі пайдаланушылардың сертификаттарында ол сыни немесе сыни емес болуы мүмкін. Кеңейту сертификат субъектісінің куәландырушы орталық болып табылатындығын не болып табылмайтындығын (CA жолағы), сондай-ақ қарастырылып отырған куәландырушы орталықтан түпкі пайдаланушыға дейін жеткізетін жолда көп дегенде (куәландырушы орталықтардың иерархиялық жүйеленуін қабылдай отырып) қанша куәландырушы орталықтардың болуы мүмкін екендігін айқындауға мүмкіндік береді (pathLength жолағы).

PathLength жолағы мәнінің 0 тең екендігі сертификаттың түпкі пайдаланушыларға ғана сертификаттар бере алатын куәландырушы орталыққа тиесілілігін білдіреді.

Сертификаттарда BasicContraints кеңейтуіне CA жолағы және pathLength жолағы көрсетілместен бос дәйектілік енгізіледі.

Кері қайтарылған сертификаттар тізіміне қол жеткізу нүктесі (CRL Distribution Points)

Кеңейту сыни болып табылмайды. Кеңейту осы шешімді қамтитын сертификатты шығарушы берген кері қайтарылған сертификаттардың өзекті тізімін алуға болатын хаттамалар мен желілік мекенжайларды айқындайды.

Сертификаттау орталықтары туралы ақпаратқа қол жеткізу (AuthorityInformationAccess)

Кеңейту сыни болып табылмайды. Жолақта деректердің және сертификатында осы кеңейту орын алған сертификат шығарушы көрсететін қызметтердің қалай берілетіні көрсетіледі. Егер осы кеңейту орын алған болса, ол әдетте куәландырушы орталықтың сертификаты файлының URL мекенжайын және осы мекенжай көрсетілген сертификаттың мәртебесін OCSP тексеру қызметтерінің URL мекенжайын қамтиды.

Алгоритмнің сәйкестендіргіші

SignatureAlgorithm жолағы Куәландырушы орталық сертификатқа енгізетін ЭЦҚ-ны іске асыру үшін қолданылатын алгоритмді сипаттайтын криптографиялық алгоритмнің сәйкестендіргішін қамтиды.

СҮТ қызметінің КО-сы беретін сертификаттар үшін жолақтың мәні:

id-tc26-gost3410-2012-512 OBJECT IDENTIFIER ::= id-tc26-signwithdigest-gost3410-2012-512 OBJECT IDENTIFIER ::= { iso(1) member-body(2) ru(643) rosstandart(7) tc26(1) algorithms(1) signwithdigest(3) gost3410-2012-512(3) }

Атаулар нысандары

СҮТ қызметінің КО-сы баспагердің және СҮТ қызметі КО-сының Регламентінде сипатталған қағидаларға сәйкес құрылатын субъектінің атауын қамтитын сертификаттар береді.

Сертификаттар саясаттарының сәйкестендіргіштері

Сертификат саясаты сертификаттар беретін СҮТ қызметінің КО-сы іске асыратын сертификат саясаты туралы PolicyInformation (сәйкестендіргіш, электрондық мекенжай) түріндегі ақпаратты қамтиды – кеңейту сыни болып табылмайды. СҮТ қызметінің КО-сы беретін сертификаттарда саясаттардың мынадай сәйкестендіргіштері болуы мүмкін:

iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id -_____(X) … – сертификат мәртебелері қызметінің сертификаты саясаты;

iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id -_____(X) … – уақыт штамптары қызметінің сертификаты саясаты;

iso(1) member-body(2) ru(643) _____(X) id ЕЭК (XXX) id-____(X) id-_____(X) id -_____(X) … – сертификаттау әкімшілігінің сертификаты саясаты. Кері қайтарылған сертификаттардың тізімі (CRL) дәйекті үш жолақтан тұрады. Бірінші жолақта (tbsCertList) кері қайтарылған сертификаттар туралы ақпарат, екінші және үшінші жолақтарда (signatureAlgorithm және signatureValue) – тиісінше тізімге қол қою үшін қолданылған алгоритмнің тұрпаты және сертификатқа куәландырушы орталық қоятын ЭЦҚ туралы ақпарат болады. Соңғы екі жолақтың мәні сертификат сияқты жағдайға толық сәйкес келеді. TbsCertList ақпараттық жолағы міндетті және опционалдық жолақтардың дәйектілігі болып табылады. Міндетті жолақ кері қайтарылған сертификаттар тізімін басып шығарушыны сәйкестендіреді, ал міндетті емес жолақтар кері қайтарылған сертификаттарды және кері қайтарылған сертификаттар тізімінің кеңейтуін қамтиды.

Кері қайтарылған сертификаттар тізімінің негізгі жолақтары мен кеңейтулерінің мәндері 2-кестеде келтірілген.

2-кесте

Жолақтың атауы	**Мән немесе мәнді шектеулер**
Version (нұсқа)	Version 2
Signature Algorithm (қолтаңба алгоритмі)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (баспагер, DN атауы)	Common Name (CN) = СҮТ қызметінің КО-сы, Organization (O) = ЕЭК, Organization Unit (OU) = ИТ, Country (C) = RU
thisUpdate	кері қайтарылған сертификаттарды шығару күні және уақыты
nextUpdate	кері қайтарылған сертификаттардың кезекті тізімін шығару күні және уақыты
revokedCertificates (Кері қайтарылған сертификаттар)	кері қайтарылған сертификаттар туралы ақпарат, сертификатқа қатысты әрбір жазба мынадай жолақтарды қамтиды: userCertificate - кері қайтарылған сертификаттың сериялық нөмірі, revocationDate – сертификатты кері қайтару күні, crlEntryExtensions - кері қайтарылған сертификаттардың тізіміне кеңейтілген қол жетімділік (кері қайтарылған сертификаттар туралы қосымша ақпаратты қамтиды - опционалды), CRLReason (сертификатты кері қайтару себебі туралы ақпаратты қамтиды – КСТ негізгі жолақтары және кеңейтулері – опционалды) жоғарыда санамаланған жолақтар туралы ақпарат осы кестенің келесі үш жолында жазылған
userCertificate (сертификат)	кері қайтарылған сертификаттың сериялық нөмірі
revocationDate (Кері қайтарылған күні)	сертификатты кері қайтару күні және уақыты
CRLReason (Кері қайтару себебі)	сертификатты кері қайтару себебі. Жол берілетін мәндер: keyCompromise; cessationOfOperation.
Extensions	сертификатты пайдаланумен байланысты қосымша ақпаратты айқындайтын кеңейтулер жиынтығы (міндетті кеңейтулер: authorityKeyIdentifier; crlNumber)
Signature (қолтаңба)	КСТ қолтаңбасы RFC 5280 айқындалған талаптарға сәйкес генерацияланады және кодталады

Нұсқа нөмірі

СҮТ қызметінің КО-сы шығаратын КСТ X.509 v2 сәйкес келеді.

КСТ кеңейтулері

CRL көптеген кеңейтулерінің арасында екеуі маңызды болып табылады, олардың біріншісі (AuthorityKeyIdentifier жолағы) кері қайтарылған сертификаттардың тізіміне қол қою үшін қолданылатын ЭЦҚ кілтіне сәйкес келетін ЭЦҚ-ны тексеру кілтін

сәйкестендіруге мүмкіндік береді, ал екіншісі (cRLNumber жолағы) куәландырушы орталық шығаратын CRL тізімінің біртіндеп ұлғайтылатын нөмірін қамтиды (осы кеңейтудің арқасында тізімді пайдаланушы бір CRL-дің екінші CRL-ді алмастырғанын айқындай алады).

OCSP шаблоны

Сертификаттың мәртебесін жедел режимде тексеру хаттамасын (OCSP) куәландырушы орталықтар қолданады және ол сертификаттардың жай-күйін айқындауға мүмкіндік береді. СМТС сұрау салулары мен жауаптарының құрылымы RFC 6960 сәйкес келеді. Осыған байланысты нұсқаның бірден бір шешілген нөмірі 0 болып табылады (бұл v1 нұсқасына сәйкес келеді). СҮТ қызметі КО-сының СМТС-ы авторланған жауапкер режимінде жұмыс істейді.

СМТС серверінің сертификаты RFC 5280-де айқындалған extKeyUsage атауындағы кеңейтуді қамтуға тиіс. Осы кеңейту сыни ретінде белгіленуге тиіс және ол куәландырушы орталық сертификатты OCSP серверіне бере отырып өз қолтаңбасымен өзінің атынан осы орталықтың клиенттері сертификаттарының мәртебесі туралы куәліктерді беру құқығының өзіне берілуі фактісін растайтынын білдіреді.

Сертификатта сертификаттың мәртебесін тексеру орталығының серверімен байланысу тәсілі туралы ақпарат та қамтылуы мүмкін. Бұл ақпарат AuthorityInfoAccess кеңейту жолағында бар.

Сертификаттың мәртебесі туралы ақпарат SingleResponse құрылымының certStatus жолағына енгізіледі. Ол СҮТ қызметі КО-сының Регламентінде айқындалған үш кеңейтілген мәннің біреуін қабылдауы мүмкін.

OCSP сұрау салуының шаблоны

OCSP-сұрау салу RFC 6960 сәйкес ASN.1-құрылымын қабылдайды және оның мынадай шектеулері болады:

TbsRequest құрылымының requestExtensions жолағында кеңейтулердің тізімі бар. Бұл тізімде ocspNonce (OID 1.3.6.1.5.5.7.48.1.2) кеңейтуі ғана болуға тиіс.

Дара сұрау салуға арналған кеңейтулердің тізімін қамтитын tbsRequest құрылымының singleRequestExtensions міндетті емес жолағы болмауға тиіс.

Егер OCSP Request құрылымының optionalSignature жолағы берілсе, онда оған мынадай шектеулер қойылады:

signatureAlgorithm жолағы "МЕМСТ Р 34.11/34.10-2012" (OID 1.2.643.7.1.1.3.3) мәнін қабылдауға тиіс;

certs жолағына OCSP сұрау салуының ЭЦҚ-ны тексеру үшін сертификат енгізілуге тиіс. Бұдан басқа, tbsRequest құрылымындағы requestorName жолағы міндетті түрде қатысуға және ол CommonName (объективтік сәйкестендіргіш - 2.5.4.3) элементін қамтитын directoryName құрылымын білдіруге тиіс.

OCSP жауабының шаблоны

OCSP-жауап RFC 6960 сәйкес ASN.1-құрылымын қабылдайды және оның мынадай шектеулері болады.

ResponseType жолағында 1.3.6.1.5.5.7.48.1.1 мәндері бар жауап түріндегі объективтік сәйкестендіргіш болады. Response жолағында BasicOCSPResponse құрылымы бар.

Егер тиісті OCSP сұрау салуында ocspNonce кеңейтуі қатысқан жағдайда, онда OCSP-жауапта ResponseData құрылымының responseExtensions міндетті емес жолағы ұқсас мәні бар ocspNonce кеңейтуін қамтитын болады.

SignatureAlgorithm жолағы "МЕМСТ Р 34.11/34.10-2012" (OID 1.2.643.7.1.1.3.3) мәнін қабылдайды.

Certs сертификаттар тізімінде ЭЦҚ-ны тексеру үшін қажетті СМТС сертификаты бар.

SingleResponse құрылымының OCSP-жауап кеңейтуін қамтуы мүмкін singleExtensions міндетті емес жолағы жоқ.

Уақыт штамптары шаблоны

СҮТ қызметі КО-сының УШС осы мақсат үшін арнайы резервтелген ЭЦҚ кілтінің көмегімен өзіне берілетін ЭЦҚ-мен уақыт штамптарына қол қояды. RFC 5280 ұсынымына сәйкес олармен үйлесетін УШС ЭЦҚ-ны тексеру кілттерінің сертификаттары сыни ретінде белгіленген кілттің (ExtKeyUsage) жол берілетін тар қолданысын нақтылайтын жолақты қамтиды. Бұл сертификатты УШС-ның пайдалануы мүмкіндігін және ол берілетін уақыт штамптарында қалыптастыру үшін ғана пайдаланатынын білдіреді.

СҮТ қызметі КО-сының УШС берген уақыт штампында SignedData құрылымына енгізілген (RFC 2630 сәйкес), УШС қол қойған және ContentInfo құрылымында бекітілген уақыт штампы туралы ақпарат (TSTInfo құрылымы) бар. СҮТ қызметі КО-сының УШС беретін уақыт штамптары RFC 3161 сәйкес келеді.

TSP сұрау салуының шаблоны

TSP-сұрау салу RFC 2630 сәйкес ASN.1-құрылымын білдіреді және оның мынадай шектеулері болады.

TimeStampReq құрылымының reqPolicy міндетті емес жолағында базалық саясаттың объективтік сәйкестендіргіші (OID = 0.4.0.2023.1.1) болмауға не ол қамтылуға тиіс.

nonce міндетті емес жолағында кездейсоқ генерацияланған 64-биттік мән болмауға не ол қамтылуға тиіс.

TSP жауабының шаблоны

TSP-жауап TSP-сұрау салу RFC 2630 сәйкес ASN.1-құрылымын білдіреді және оның мынадай шектеулері болады.

SignedData құрылымының digestAlgorithms жолағы "512 ұзындығымен МЕМСТ 34.11-2012" (OID 1.2.643.7.1.1.2.3) мәнін қабылдайды;

егер TSP сұрау салуда TimeStampReq құрылымының certReq міндетті емес жолағында true мәні болса, SignedData құрылымының certificates міндетті емес жолағы TSP қызметінің сертификатын қамтитын болады.

SignedData құрылымының crls міндетті емес жолағы болмауға тиіс.

TSTInfo құрылымының policy жолағында базалық саясаттың объективтік саясаты (OID = 0.4.0.2023.1.1) болуға тиіс.

егер тиісті TSP-сұрау салуда nonce міндетті емес жолағы болған жағдайда, TSP-жауапта TSTInfo құрылымының nonce міндетті емес жолағы да соған ұқсас мәнді иеленетін болады.

TSTInfo құрылымының tsa міндетті емес жолағы жоқ.

TSTInfo құрылымының extensions міндетті емес жолағы жоқ.

SignerInfo құрылымының digestAlgorithm жолағы "512 ұзындығымен МЕМСТ Р 34.11-2012" мәнін (OID 1.2.643.7.1.1.2.3) қабылдайды.

SignerInfo құрылымының signedAttrs жолағы мынадай объектілерді қамтитын болады: қол қойылатын мөлшердің тұрпаты (OID 1.2.840.113549.1.9.16.1.4 (уақыт штампы)), уақыт штампы хеш-функциясының мәні, уақыт штампы қызметінің сертификаты туралы ақпарат;

SignerInfo құрылымының signatureAlgorithm жолағы "512 ұзындығымен МЕМСТ Р 34.10-2.12" мәнін қабылдайды.

Еуразиялық экономикалық
одақтың интеграцияланған
ақпараттық жүйесінің сенім
білдірілген үшінші тарапы
қызметі куәландырушы
орталығының регламентіне
№ 2 ҚОСЫМША

Құжаттар түпнұсқалылығының негізгі белгілерінің ТІЗБЕСІ

1. Паспорт:

паспорттың бланкісі бекітілген және қолданыстағы нысанға сәйкес келеді;

барлық міндетті деректемелері, мөрлері, мөртабандары бар;

паспорттың қолданылу мерзімі өткен жоқ;

лауазымды адамдардың қолтаңбалары бар;

туған күні және паспорттың берілген күні сәйкес келеді;

паспортты беру жүргізілген өңір туралы жазбалар азаматтың сол сәтте тұрған жері бойынша тіркеу мөртабанына сәйкес келеді және құжаттағы фотосурет (соның ішінде фотосуретте бейнеленген адамның шамамен алғандағы жасы құжатта көрсетілгенге сәйкес келеді) ұсынушыға сәйкес келеді.

2. Сенімхат және бұйрықтардың көшірмелері:

мөр бедерінде грамматикалық қателер, симметриялы емес орналасқан мәтін, штрихтардың қисықтығы, иректігі, басу бейнесінің жалпы солғындығы, қағаздың деформациясы, қаріптер мен цифрлардың оңайлатылған суреті, кертпесіз қаріптер мен цифрлар, бұрышты құрылысы бар сопақшалар мен жартылай сопақшалар жоқ.

Еуразиялық экономикалық
одақтың интеграцияланған
ақпараттық жүйесінің сенім
білдірілген үшінші тарапы
қызметі куәландырушы
орталығының регламентіне
№ 3 ҚОСЫМША

Сертификат жасауға және беруге арналған өтініштің НЫСАНЫ

СҮТ қызметі КО-сының басшысына

_____

115114, Мәскеу қ., Летниковская к-сі, 2-үй, 1-құр.

_____

(басшы лауазымының атауы)

_____

(ұйымның толық атауы)

_____

(басшының Т. А. Ә.)

/

/

ЭЦҚ-ны тексеру кілтінің сертификатын дайындауға ӨТІНІШ

1. ЭЦҚ кілтін және ЭЦҚ-ны тексеру кілтін жасауды және осы өтініште көрсетілген деректерге сәйкес ЭЦҚ-ны тексеру кілтінің сертификатын дайындауды сұраймын:

Ұйымның атауы (қысқ.)	
Т. А. Ә. (толық):	
Туған күні	
Туған жері (толық)	
Жынысы	ер әйел
Паспорт деректері (серия, нөмір):	
(бөлімше коды)	
(берілген күні)	
Лауазымы:	

Бөлімше:	
e-mail/телефон:	
Заңды мекенжайы (толық):	
Мекенжай бойынша жұмыс орны:	

Сертификаттың тағайындалуы:

☐ СҮТС серверінің сертификаты

☐ УШС серверінің сертификаты

☐ СМТС серверінің сертификаты

СҮТ қызметінің Куәландырушы орталығы Регламентінің және оған қосымшаның талаптарымен таныстым және оның барлық ережелерін сақтауға міндеттенемін.

ЭЦҚ-ны тексеру кілті сертификатының иесі				
		[жеке қолы]		Т.А.Ә.

2. Мәліметтер түпнұсқа құжаттардың негізінде ұсынылды және дұрыс болып табылады.

(Ұйым басшысының лауазымы)		(қолы)		(Т.А.Ә.)
" " ж.				
М.О.				

Еуразиялық экономикалық одақтың интеграцияланған ақпараттық жүйесінің сенім білдірілген үшінші тарапы қызметі куәландырушы орталығының регламентіне № 4 ҚОСЫМША

Сертификаттың күшін жоюға арналған өтініштің НЫСАНЫ

	СҮТ қызметі КО-сының басшысына
	115114, Мәскеу қ., Летниковская к-сі, 2-үй, 1-құр.
	(басшы лауазымының атауы)
	(ұйымның толық атауы)
	(басшының Т. А.Ә.)

	/
	/

Қол кілтінің сертификатын кері қайтаруға ӨТІНІШ

Сізден сертификаттың күшін жоюды,
Сертификаттың тағайындалуы:

☐ СҮТС серверінің сертификаты
☐ УШС серверінің сертификаты
☐ СМТС серверінің сертификаты

және күші жойылған сертификатты кері қайтарылған сертификаттардың тізіміне қосуды сұраймын:

(Лауазымы, Т.А.Ә. толық)				
(Күшін жою себебі)				
Сертификат №				
	(Сериялық нөмірі)			
(Ұйым басшысының лауазымы)		(қолы)		(Т.А.Ә.)
"___" _____ 20__ ж.				
М.О.				

Еуразиялық экономикалық одақтың интеграцияланған ақпараттық жүйесінің сенім білдірілген үшінші тарапы қызметі куәландырушы орталығының регламентіне № 5 ҚОСЫМША

Сертификат алуға сенімхаттың НЫСАНЫ

	СҮТ қызметі КО-сының басшысына
	115114, Мәскеу қ., Летниковская к-сі, 2-үй, 1-құр.
	(басшы лауазымының атауы)
	(ұйымның толық атауы)
	(басшының Т.А.Ә.) /

	/

ЭЦҚ-ны тексеру кілтінің сертификатын алуға СЕНІМХАТ

_____

_____

_____

_____

_____ сұраймын

Сенімхат берілетін адам туралы мәліметтер:

Т. А. Ә. (толық):	
Туған күні	
Туған жері (толық)	
Жынысы	ер әйел
Паспорт деректері (сериясы, нөмірі):	
(бөлімшенің коды)	
(берілген күні)	
Лауазымы:	
Бөлімше:	
e-mail/телефон:	
Заңды мекенжайы (толық):	
Мекенжай бойынша жұмыс орны:	

Атына сенімхат берілетін адам				
		жеке қолы		Т.А.Ә.

2. Мәліметтер түпнұсқа құжаттардың негізінде ұсынылды және дұрыс болып табылады.

(Ұйым басшысының лауазымы)		(қолы)		(Т.А.Ә.)
"_____"_____ _____20___ж.				
М.О.				