1-тиркеме

Электрондук колтамганын квалификацияланган сертификатынын формасына
ТАЛАПТАР

1-глава. Жалпы жоболор

1. Электрондук кол тамганын квалификацияланган сертификатынын формасына ушул талаптар (мындан ары – Талаптар) аккредиттелген күбөлөндүрүүчү борбор тарабынан колтамга текшерүү ачкычынын квалификацияланган сертификаттарын түзүү шарттарын аныктоо үчүн арналган.

2. Ушул Талаптар “Электрондук колтамга жөнүндө” Кыргыз Республикасынын мыйзамына (мындан ары – мыйзам) ылайык жана “Электрондук колтамганы пайдаланууга байланышкан айрым маселелер жөнүндө” Кыргыз Республикасынын Өкмөтүнүн 2019-жылдын 31-декабрындагы № 742 токтомунун 2-пунктун аткаруу максатында иштелип чыкты.

3. Ушул Талаптар Кыргыз Республикасынын мамлекеттик сырларына таандык маалыматты коргоо каражаттарына жайылтылбайт.

4. Ушул Талаптарда мыйзамга ылайык төмөнкүдөй түшүнүктөр колдонулат:

1) электрондук колтамга (мындан ары – ЭКТ) – электрондук формадагы башка маалыматка кошулган жана (же) ага логикалык жактан байланышкан, атынан маалыматка кол койгон адамды аныктоо үчүн пайдаланылуучу электрондук формадагы маалымат;

2) колтамга текшерүү ачкычынын сертификаты – күбөлөндүрүүчү борбор берген жана колтамга текшерүү ачкычы колтамга текшерүү ачкычынын сертификат ээсине таандык экенин тастыктаган электрондук документ же кагаз түрүндөгү документ;

3) колтамга текшерүү ачкычынын квалификацияланган сертификаты (мындан ары – квалификацияланган сертификат) - аккредиттелген күбөлөндүрүүчү борбор же аккредиттелген күбөлөндүрүүчү борбордун ишенимдүү адамы, же болбосо башкы (түпкү) күбөлөндүрүүчү борбордун функцияларын жүзөгө ашыруучу, электрондук колтамганы пайдалануу чөйрөсүндөгү ыйгарым укуктуу аткаруу бийлик органы тарабынан берилген колтамга текшерүү ачкычынын сертификаты;

4) колтамга текшерүү ачкычынын сертификат ээси – мыйзамда белгиленген тартипте, күбөлөндүрүүчү борбор колтамга текшерүү ачкычынын сертификатын берген адам;

5) колтамга ачкычы – электрондук колтамганы түзүүгө арналган символдордун уникалдуу ырааттуулугу;

6) колтамга текшерүү ачкычы – колтамга ачкычы менен бир мааниде байланышкан жана электрондук колтамганын аныктыгын текшерүүгө

(мындан ары – электрондук колтамганы текшерүү) арналган символдордун уникалдуу ырааттуулугу;

7) күбөлөндүрүүчү борбор (мындан ары – КБ) – колтамга текшерүү ачкычынын сертификаттарын түзүү жана берүү боюнча ишти жүзөгө ашыруучу юридикалык жак же жеке ишкер;

8) күбөлөндүрүүчү борборду аккредиттөө – күбөлөндүрүүчү борбордун мыйзамда белгиленген талаптарга ылайык келе тургандыгын электрондук колтамганы пайдалануу чөйрөсүндө ыйгарым укук берилген аткаруу бийлик органынын таануусу;

9) электрондук колтамга каражаттары – төмөнкүдөй функциялардын эч болбогондо бирин: электрондук колгамганы түзүүнү, электрондук колтамганы текшерүүнү, колтамганын ачкычтарын жана колтамганы текшерүү ачкычтарын түзүүнү ишке ашыруу үчүн пайдаланылуучу шифрлөөчү (криптографиялык) каражаттар;

10) күбөлөндүрүүчү борбордун каражаттары – колтамга текшерүү ачкычынын сертификатын түзүү, сактоо жана берүү функцияларын ишке ашыруу, ошондой эле колтамга текшерүү ачкычынын сертификаттарынын реестрин жүргүзүү үчүн пайдаланылуучу программалык жана (же) аппараттык каражаттар.

2-глава. Квалификацияланган сертификаттын формасына талаптар

5. Ушул Талаптар квалификацияланган сертификаттын милдеттүү жана кошумча талааларын (мындан ары – квалификацияланган сертификаттын формасы) аныктайт.

6. квалификацияланган сертификаттын кошумча талааларын дайындоо жана алардын квалификациялуу сертификатта жайгашуусу КБ каражаттарын иштеп чыгууга (модернизациялоого) техникалык тапшырмаларда аныкталат.

7. Мыйзамга ылайык квалификацияланган сертификатта төмөнкү маалыматтар камтылууга тийиш:

- квалификацияланган сертификаттын уникалдуу номери;
- квалификацияланган сертификаттын аракетинин башталган жана аяктаган күндөрү;
- квалификацияланган сертификат ээсинин – жеке жактын фамилиясы, аты жана атасынын аты (эгерде бар болсо), төрөлгөн жери жана күнү, же болбосо квалификациялуу сертификат ээсинин – юридикалык жактын аткаруу органынын аталышы (фирмалык аталышы), каттоо номери жана катталган жана (же) иш жүзүндө жайгашкан жери;
- юридикалык жак үчүн – квалификацияланган сертификат ээси салык төлөөчүнүн идентификациялык номери (мындан ары – ИНН) же жеке жак үчүн – квалификацияланган сертификат ээси салык төлөөчүнүн идентификациялык номери (мындан ары – ПИН);
- колтамга текшерүү ачкычы;

- колтамга ачкычын, колтамга текшерүү ачкычын жана квалификацияланган сертификатты түзүү үчүн пайдаланылган электрондук колтамга каражаттарынын жана күбөлөндүрүүчү борбордун каражаттарынын аталыштары, ошондой эле аталган каражаттардын мыйзамга ылайык белгиленген талаптарга туура келүүсүн тастыктоочу документтин реквизиттери;

- квалификацияланган сертификатты берген күбөлөндүрүүчү борбордун аталышы жана жайгашкан жери, күбөлөндүрүүчү борбордун квалификацияланган сертификатынын номери жана бул борборду аккредиттөө тууралуу күбөлүктүн реквизиттери;

- квалификацияланган сертификатты пайдалануудагы чектөөлөр (эгерде чектөөлөр белгиленсе);

- өтүнмө берүүчү тууралуу башка маалыматтар (өтүнмө берүүчүнүн талабы боюнча).

8. Эгерде өтүнмө ээси анын үчүнчү жактардын атынан аракеттерди жүргүзүү укугун тастыктоочу документтер аккредиттелген күбөлөндүрүүчү борборго берсе, өтүнмө берүүчүнүн мындай укуктуулуктары жана алардын колдонулуу мөөнөтү тууралуу күбөлөндүрүүчү маалыматтар квалификацияланган сертификатка киргизилет.

8[1]. Өтүнмө берүүчүгө квалификацияланган сертификат берген аккредиттелген күбөлөндүрүүчү борборго берилген квалификацияланган сертификат жокко чыгарылган учурда, ошондой эле күбөлөндүрүүчү борбордун аккредиттөөсү жокко чыгарылган же анын мөөнөтү бүткөн учурда, арыз берүүчүгө аккредиттелген күбөлөндүрүүчү борбор берген квалификацияланган сертификаттын колдонулуусу токтотулат.

8[2]. Квалификацияланган сертификат ээси колтамга ачкычынын купуялуулугу бузулгандыгын божомолдоого негиздер болгондо, бул ачкычты колдонууну токтотууга жана квалификацияланган сертификат берген күбөлөндүрүүчү борборго бул сертификаттын колдонулуусун токтотуу үчүн дароо кайрылууга милдеттүү.

3-глава. Квалификацияланган сертификаттын талаасынын жайгашуусунун тартибине талаптар

9. Квалификацияланган сертификаттын талаасынын жайгашуусунун тартибине талаптар ачык системалардын аутентификациясынын негизине (Талаптардын 6-главасынын 1-пунктун караңыз), ачык ачкычтын сертификатынын жана атрибут сертификатынын түзүмүнө (Талаптардын 6-главасынын 2-пунктун караңыз), сертификаттын профилине жана жокко чыгарылган сертификаттардын тизмесине (Талаптардын 6-главасынын 3-пунктун караңыз) ылайык белгиленет.

10. 1-версиядагы абстракттуу синтаксистик нотациянын өзгөчөлүгүнө ылайык аныкталган электрондук документ түрүндөгү квалификацияланган сертификаттын түзүмү (Талаптардын 6-главасынын 4-пунктун караңыз) төмөнкүдөй жалпы түргө ээ болушу керек:

```
Certificate:: = SIGNED { SEQUENCE {
    version                 [0]  Version DEFAULT v1,
    serialNumber                 CertificateSerialNumber,
    signature                    AlgorithmIdentifier,
    issuer                       Name,
    validity                     Validity,
    subject                      Name,
    subjectPublicKeyInfo         SubjectPublicKeyInfo,
    issuerUniqueIdentifier  [1]  IMPLICIT UniqueIdentifier
                        OPTIONAL,
    subjectUniqueIdentifier [2]  IMPLICIT UniqueIdentifier
                        OPTIONAL,
    extensions              [3]  Extensions OPTIONAL }}
SIGNED { ToBeSigned }:: = SEQUENCE {
    toBeSigned                   ToBeSigned,
    COMPONENTS OF                SIGNATURE { ToBeSigned }}
SIGNATURE { ToBeSigned }::= SEQUENCE {
    algorithmIdentifier          AlgorithmIdentifier,
    encrypted                    ENCRYPTED-HASH { ToBeSigned }}
ENCRYPTED-HASH {ToBeSigned }:: = BIT STRING (CONSTRAINED BY
                             { ToBeSigned }).
```

11. AlgorithmIdentifier (алгоритмдин идентификатору) талаасы алгоритмдин идентификаторун камтыйт, аны колдонуу менен аккредиттелген күбөлөндүрүүчү борбор, аккредиттелген күбөлөндүрүүчү борбордун ишенимдүү жагы же ыйгарым укуктуу орган ушул квалификацияланган сертификаттын электрондук колтамгасын түзгөн.

Криптографиялык алгоритмдин параметрлери кошумча көрсөтүлүшү мүмкүн:

```
AlgorithmIdentifier::= SEQUENCE {
    algorithm ALGORITHM.&id ( { SupportedAlgorithms } ),
    parameters ALGORITHM.&Type ({ SupportedAlgorithms }
                      { @algorithm } ) OPTIONAL }.
```

12. Encrypted талаасы квалификацияланган сертификаттын (toBeSigned) талаасынын түзүлүштүү жыйындысынын астында аккредиттелген күбөлөндүрүүчү борбор, аккредиттелген күбөлөндүрүүчү борбордун ишенимдүү жагы же ыйгарым укуктуу орган түзгөн электрондук колтамганы камтыйт.

13. Version (версия) талаасы сертификат форматынын версия номерин камтыйт: Version::= INTEGER { v1(0), v2(1), v3(2) }.

14. Сертификат кошумчаларын колдонуу зарылдыгынан улам version талаасынын мааниси 2ге барабар болушу керек.

15. SerialNumber (сериялык номер) талаасы ушул аккредиттелген күбөлөндүрүүчү борбор, күбөлөндүрүүчү борбордун ишенимдүү жагы же ыйгарым укуктуу орган берген бардык сертификаттардын топтомунда квалификацияланган сертификат оң бүтүн санды камтууга тийиш: CertificateSerialNumber::= INTEGER.

16. Signature (колтамга) талаасы криптографиялык алгоритмдин идентификаторун камтыйт, аны колдонуу менен аккредиттелген күбөлөндүрүүчү борбор, аккредиттелген күбөлөндүрүүчү борбордун ишенимдүү жагы же ыйгарым укуктуу орган ушул квалификацияланган сертификаттын электрондук колтамгасын түзүшкөн. Ушул талаанын мазмуну algorithmIdentifier талаасынын мазмунуна туура келиши керек.

17. Issuer (басып чыгаруучу) талаасы Name түрүндө болот жана ушул квалификацияланган сертификатты түзгөн, берген аккредиттелген күбөлөндүрүүчү борборду, аккредиттелген күбөлөндүрүүчү борбордун ишенимдүү жагын же ыйгарым укуктуу органды идентификациялайт. Name түрү төмөнкүдөй сүрөттөлөт:

```
Name::= CHOICE { rdnSequence RDNSequence }
RDNSequence::= SEQUENCE OF RelativeDistinguishedName
RelativeDistinguishedName::= SET SIZE (1..MAX) OF
AttributeTypeAndValue
AttributeTypeAndValue::= SEQUENCE {
    type        AttributeType,
    value       AttributeValue }
AttributeType::= OBJECT IDENTIFIER
AttributeValue::= ANY DEFINED BY AttributeType.
```

Value талаасынын түрү атрибуттун түрү менен аныкталат, бирок жалпысынан AttributeValue катары DirectoryString түрү чыгат:

```
DirectoryString::= CHOICE {
    teletexString       TeletexString (SIZE (1..MAX)),
    printableString     PrintableString (SIZE (1..MAX)),
    universalString     UniversalString (SIZE (1..MAX)),
    utf8String          UTF8String (SIZE (1..MAX)),
    bmpString           BMPString (SIZE (1..MAX)) }
```

18. Ысымдын стандарттык атрибуттары атрибуттардын тандалган түрлөрү боюнча маалымдамада баяндалат (Талаптардын 6-главасынын 5-пунктун караңыз). Квалификацияланган сертификаттын формасын сыпаттоодо төмөнкүдөй ысымдын стандарттык атрибуттары колдонулат:

1) CommonName (толук аты-жөнү).

Ушул аталыш атрибутунун мааниси катары жеке жак үчүн – толук аты-жөнүн (эгер бар болсо) же юридикалык жак үчүн – аталышты камтыган текст сабын колдонуу керек. CommonName атрибут түрүнүн объект идентификатору 2.5.4.3 түрүнө ээ;

2) Surname (фамилия).

Ушул аталыш атрибутунун мааниси катары жеке жактын фамилиясын камтыган текст сабын колдонуу керек. Surname атрибут түрүнүн объект идентификатору 2.5.4.4 түрүнө ээ;

3) GivenName (берилген ысым).

Ушул аталыш атрибутунун мааниси жеке жактын атын жана атасынын атын (эгер бар болсо) камтыган текст сабын колдонуу керек. GivenName атрибут түрүнүн объект идентификатору 2.5.4.42 түрүнө ээ;

4) CountryName (өлкөнүн аталышы).

Ушул аталыш атрибутунун мааниси өлкөнүн эки белгиден турган кодду колдонуу керек (Талаптардын 6-главасынын 6-пунктун караңыз). CountryName атрибут түрүндөгү объект идентификатору 2.5.4.6 түрүнө ээ;

5) StateOrProvinceName (облустун аталышы).

Ушул аталыш атрибутунун мааниси Кыргыз Республикасынын тийиштүү облусунун аталышын камтыган текст сабын колдонуу керек. StateOrProvinceName атрибут түрүнүн объект идентификатору 2548 түрүнө ээ;

6) LocalityName (калктуу конуштун аталышы).

Ушул аталыш атрибутунун мааниси катары тийиштүү калктуу конуштун аталышын камтыган текст сабын колдонуу керек. болушу керек. LocalityName атрибут түрүнүн объект идентификатору 2.5.4.7 түрүнө ээ;

7) StreetAddress (көчөнүн аталышы, үйдүн номери).

Ушул аталыш атрибутунун мааниси катары көчөнүн аталышы, үйдүн номери, ошондой эле корпусту, түзүлүштү, батирди, жайды (эгер бар болсо) кошуп, тийиштүү адамдын жайгашкан жеринин дарегинин бир бөлүгүн камтыган текст сабын колдонуу керек. StreetAddress атрибут түрүнүн объект идентификатору 2.5.4.9 түрүнө ээ;

8) OrganizationName (уюмдун аталышы).

Ушул аталыш атрибутунун мааниси катары юридикалык жактын аталышын камтыган текст сабын колдондуу керек. OrganizationName атрибут түрүнүн объект идентификатору 2.5.4.10 түрүнө ээ;

9) OrganizationUnitName (уюмдун бөлүкчөсү).

Ушул аталыш атрибутунун мааниси катары юридикалык жактын бөлүкчөсүнүн аталышын камтыган текст сабын колдонуу керек. OrganizationUnitName атрибут түрүнүн объект идентификатору 2.5.4.11 түрүнө ээ;

10) Title (кызмат орду).

Ушул аталыш атрибутунун мааниси адамдын кызмат ордун камтыган текст сабын колдонуу керек. Title атрибут түрүнүн объект идентификатору 2.5.4.12 түрүнө ээ.

Квалификацияланган сертификат ээси тууралуу башка маалыматты квалификацияланган сертификатка киргизүү үчүн тандалган атрибут түрлөрүнүн маалымдамасында сүрөттөлгөн аталыштын стандарттык атрибуттарын колдонуу сунушталат.

19. Аталыштын кошумча атрибуттарына төмөнкүлөр кирет:

1) INNLE (ЮЖ ИНН)

Ушул аталыш атрибутунун мааниси катары квалификацияланган сертификаттын юридикалык жагынын салык төлөөчүсүнүн идентификациялык номерин билдирген 14 сандан турган текст сабын колдонуу керек. INNLE атрибут түрүнүн объект идентификатору 1.2.643.100.4 түрүнө ээ, INNLE атрибут түрү төмөнкүчө сүрөттөлөт: INNLE::= NUMERIC STRING SIZE 14;

INN атрибутунун түрү 1.2.643.3 болушу керек (11.1.1, төмөнкү саптар менен: САНЧЫЛЫК САПТЫН ӨЛЧӨМҮ: 14

2) PIN (ЖЖ ПИН)

Ушул аталыш атрибутунун мааниси катары квалификацияланган сертификат ээсинин персоналдык идентификациялык номерин билдирген 14 сандан турган текст сабын колдонуу керек. INN атрибут түрүнүн объект идентификатору 1.2.643.3.131.1.1 түрүнө ээ, INN атрибут түрү төмөнкүчө сүрөттөлөт: INN::= NUMERIC STRING SIZE 14;

3) DateOfBirth (туулган күнү).

Ушул аталыш атрибутунун мааниси катары "DD.MM.YYYY" форматында жеке жактын туулган күнүн камтыган текст сабын колдонуу керек. DateOfBirth атрибут түрүнүн объект идентификатору 1.3.6.1.5.5.7.9.1 түрүнө ээ;

4) PlaceOfBirth (туулган жери).

Ушул аталыш атрибутунун мааниси катары жеке жактын туулган жерин камтыган текст сабын колдонуу керек. PlaceOfBirth атрибут түрүнүн объект идентификатору 1.3.6.1.5.5.7.9.2 түрүнө ээ;

5) Description (сүрөттөө).

Ушул аталыш атрибутунун мааниси катары күбөлөндүрүүчү борборду аккредиттөө күбөлүгүнүн реквизиттерин камтыган текст сабын колдонуу керек. Description атрибут түрүнүн объект идентификатору 2.5.4.13 түрүнө ээ.

20. Validity талаасы Validity түрүнө ээ жана квалификацияланган сертификаттын жарактуулук мөөнөтүнүн башталыш жана аяктаган күнүн камтыйт. Validity түрү төмөнкүдөй сүрөттөлөт:

```
Validity::= SEQUENCE {
        notBefore       Time,
        notAfter        Time}
Time::= CHOICE {
        utcTime         UTCTime,
generalTimeGeneralizedTime }.
```

21. Subject талаасы Name түрүнө ээ жана квалификацияланган сертификат ээсин идентификациялайт.

22. SubjectPublicKeyInfo талаасы SubjectPublicKeyInfo түрүнө ээ жана квалификацияланган сертификат ээсинин электрондук колтамга текшерүү ачкычынын маанисин, ошондой эле бул ачкыч колдонулушу керек болгон криптографиялык алгоритмдин идентификаторун камтыйт:

SubjectPublicKeyInfo::=SEQUENCE{algorithm

AlgorithmIdentifier, subjectPublicKey BIT STRING }.

23. IssuerUniqueldentifier жана subjectUniqueIdentifier милдеттүү эмес талаалар UniqueIdentifier түрүнө ээ. Ушул Талаптар жогорудагы талааларды пайдаланууга талаптарды белгилебейт.

24. Квалификацияланган сертификатты колдонууга тиешелүү кошумча маалымат төмөнкүдөй толуктоолордун курамына киргизилет:

Extensions::= SEQUENCE {
extnld EXTENSION.&id ({ ExtensionSet}),
critical BOOLEAN DEFAULT FALSE,
extnValue OCTET STRING }.

Квалификацияланган сертификат ээси тууралуу квалификацияланган сертификатка аталыштын тийиштүү стандарттык атрибуттары каралбаган башка маалыматты, анын ичинде квалификацияланган сертификат ээсинин ыйгарым укуктары тууралуу маалыматты жана анын колдонуу мөөнөтүн киргизүү үчүн subjectAlternativeName кошумчалоо колдонуу сунушталат.

25. AuthorityKeyIdentifier кошумчасы (күбөлөндүрүүчү борбордун ачкычынын идентификатору) AuthorityKeyIdentifier түрүнө ээ, анын түзүмү төмөнкүдөй аныкталат:

AuthorityKeyIdentifier::= SEQUENCE {
keyIdentifier[0] KeyIdentifier OPTIONAL,
authorityCertIssuer[1] GeneralNames OPTIONAL, authorityCertSerialNumber[2] CertificateSerialNumber
OPTIONAL }.

Квалификацияланган сертификатта аккредиттелген күбөлөндүрүүчү борбордун тийиштүү квалификацияланган сертификатынын же аккредиттелген күбөлөндүрүүчү борбордун ишенимдүү жагынын же баштапкы квалификацияланган сертификатты түзгөн ыйгарым укуктуу органдын номерин authorityCertSerialNumber талаасына киргизүү менен authorityKeyIdentifier кошумчасын колдонуу керек. AuthorityKeyIdentifier кошумчалоо түрүнүн объект идентификатору 2.5.29.35 түрүнө ээ.

26. KeyUsage кошумчасы квалификацияланган сертификаттын subjectPublicKeyInfo талаасында камтылган электрондук колтамга текшерүү ачкычын колдонуу жаатын аныктайт. KeyUsage кошумчасы KeyUsage түрүнө ээ, анын түзүмү төмөнкүдөй түрдө аныкталат:

KeyUsage::= BIT STRING {
digitalSignature (0),
ontentCommitment (1),
keyEncipherment (2),
dataEncipherment (3),
keyAgreement (4),
keyCertSign (5),
cRLSign (6),
encipherOnly (7),
decipherOnly (8) }.

Нөл битиндеги “1” мааниси ачкычты колдонуу жааты квалификацияланган сертификаттардан башка электрондук документтер боюнча электрондук колтамга текшерүүнү жана бүтүндүктү аутентификациялоо же контролдоо жол-жобосун аткаруу үчүн багытталган, алардын жарактуулук мөөнөтү аяктаганга чейин алардын иш-аракетин белгилүү бир учурда күбөлөндүрүүчү борбор токтоткон электрондук колтамга текшерүү ачкычынын квалификацияланган сертификаттарынын уникалдуу номерлеринин тизмеси (мындан ары – жокко чыгарылган сертификаттардын тизмеси) камтылгандыгын билдирет.

Биринчи биттеги “1” мааниси ачкычты колдонуу жаатына квалификацияланган сертификаттардан жана жокко чыгарылган сертификат тизмелеринен башка электрондук документтерде электрондук колтамга текшерүүнү камтыганын билдирет, аларга карата кол койгон адамдын өз иш-аракетинен баш тартууга мүмкүн эместигин камсыздоо милдети коюлган.

Экинчи биттеги “1” мааниси ачкычты колдонуу жаатына купуя же жашыруун ачкычтарды шифрлөө кирет, мисалы, аларды коргоп жеткирүү максатында.

Үчүнчү биттеги “1” мааниси ачкычты колдонуу жааты симметриялык криптографияны кошумча колдонбостон колдонуучунун маалыматтарын түздөн-түз шифрлөө камтылганын билдирет.

Төртүнчү биттеги “1” мааниси ачкычты колдонуу жааты ачкычтарды макулдашууну камтыганын билдирет.

Бешинчи биттеги “1” мааниси ачкычты колдонуу жааты квалификацияланган сертификаттагы колтамганы текшерүү камтылганын билдирет.

Алтынчы биттеги “1” мааниси ачкычты колдонуу жааты жокко чыгарылган сертификаттардын тизмесиндеги колтамганы текшерүү камтылганын билдирет.

Жетинчи биттеги “1” мааниси ачкычты колдонуу жааты ачкычтарды макулдашуу учурунда маалыматты шифрлөөнү камтыйт (муну менен катар төртүнчү битте маани “1” болушу керек).

Сегизинчи биттеги “1” мааниси ачкычты колдонуу жааты ачкычтарды макулдашуу учурунда маалыматтын ачыкка чыгуусун камтыйт (муну менен катар төртүнчү битте маани “1” болушу керек).

KeyUsage кошумчалоонун объект идентификатору 2.5.29.15 түрүнө ээ.

27. CertificatePolicies кошумчалоо ага ылайык квалификацияланган сертификат колдонулушу керек болгон сертификациялоо саясатын негиздөөгө багытталган. CertificatePolicies кошумчалоону сүрөттөгөн сертификаттоо саясатын көрсөтүүгө арналган. CertificatePolicies кошумчасын CertificatePoliciesSyntax түрү төмөнкүдөй түрдө аныкталат:

```
CertificatePoliciesSyntax::=    SEQUENCE   SIZE   (1..MAX)   OF
PolicylInformation PolicyInformation::= SEQUENCE {
    policyIdentifier    CertPolicyId,
    policyQualifiers    SEQUENCE SIZE (1..MAX) OF
```

```
                PolicyQualifierInfo OPTIONAL}
CertPolicyId::= OBJECT IDENTIFIER
PolicyQualifierInfo::= SEQUENCE {
    policyQualifierId    PolicyQualifierId,
    qualifier            ANY DEFINED BY policyQualifierld }
    PolicyQualifierId::= OBJECT IDENTIFIER.
```

CertificatePolicies кошумчалоо объект идентификатору 2.5.29.32 түрүнө ээ.

28. Квалификацияланган сертификатта квалификацияланган сертификат ээси колдонгон электрондук колтамга каражатынын аталышын көрсөтүү үчүн объект идентификатору 1.2.643.100.111 түрүнө ээ болгон UTF8String SIZE(1..200) түрүндөгү subjectSignTool өзгөчө маанилүү эмес кошумчалоо колдонулушу керек.

29. Квалификацияланган сертификатта электрондук колтамга каражатынын жана электрондук колтамга ачкычын, электрондук колтамга текшерүү ачкычын, квалификацияланган сертификатты, ошондой эле жогорудагы каражаттардын Кыргыз Республикасынын мыйзамдарында белгиленген талаптарга шайкештигин тастыктаган документтин реквизиттерин түзүү үчүн колдонулган аккредиттелген күбөлөндүрүүчү борбордун каражатынын аталышын төмөнкүдөй сунуштамага ээ IssuerSignTool түрүндөгү issuerSignTool өзгөчө маанилүү эмес кошумчалоо колдонулууга тийиш:

```
IssuerSignTool::= SEQUENCE {
signTool          UTF8String SIZE(1..200),
cATool            UTF8String SIZE(1..200),
signToolCert        UTF8StringSIZE(1..100),
cAToolCert        UTF8StringSIZE(1..100)}.
```

SignTool сап талаасында электрондук колтамга ачкычын, электрондук колтамга текшерүү ачкычын жана квалификацияланган сертификатты түзүү үчүн колдонулган электрондук колтамга каражатынын толук аталышы камтылууга тийиш.

CATool сап талаасында электрондук колтамга ачкычын, электрондук колтамга текшерүү ачкычын жана квалификацияланган сертификатты түзүү үчүн колдонулган аккредиттелген күбөлөндүрүүчү борбордун каражатынын толук аталышы камтылууга тийиш.

Sign ToolCert сап талаасында электрондук колтамга ачкычын, электрондук колтамга текшерүү ачкычын түзүү үчүн колдонулган мыйзамга ылайык белгиленген талаптарга шайкештигин тастыктаган корутундунун реквизиттери камтылууга тийиш (мындан ары – электрондук колтамга каражатынын шайкештигин тастыктоо тууралуу корутунду).

CAToolCert сап талаасында квалификацияланган сертификатты түзүү үчүн колдонулган мыйзамга ылайык белгиленген талаптарга күбөлөндөрүүчү

борбордун каражаттарынын шайкештигин тастыктаган корутундунун реквизиттери камтылууга тийиш (мындан ары – күбөлөндүрүүчү борбордун каражаттарынын шайкештигин тастыктоочу корутунду).

IssuerSignTool түрүндөгү объек идентификатору 1.2.643.100.112. түрүнө ээ.

30. Кагаз түрүндөгү документте квалификацияланган сертификаттын түрү төмөнкү талаптарга жооп бериши керек:

- квалификацияланган сертификаттын талааларын адам өздөштүрө турган түрдө көрсөтүү;

- квалификацияланган сертификатта камтылган маалыматты мамлекеттик жана расмий тилде кириллицада көрсөтүү;

- электрондук жана кагаз түрүндө документ түрүндөгү квалификацияланган сертификаттын шайкештигин расмий түрдө жол-жобону жүргүзүү үчүн ылайыктуулугун камсыздоо.

Кагаз түрүндөгү квалификацияланган сертификатта бардык квалификацияланган сертификаттар үчүн белгиленген талаа маанилерин алып салууга жол берилет (мисалы, version талаасы v3ге шайкеш келген 2 мааниге ээ).

Кагаз түрүндөгү квалификацияланган сертификатта түрдүү талааларда кайталанган маалыматты бир гана жолу көрсөтүүгө жол берилет (мисалы, algorithmIdentifier жана signature).

Жеке жактар үчүн кагаз түрүндөгү квалификацияланган сертификаттын жалпы түрү ушул Талаптардын 4-главасында келтирилген.

Юридикалык жактар үчүн кагаз түрүндөгү квалификацияланган сертификаттын жалпы түрү ушул Талаптардын 5-главасында каралган.

4-глава. Жеке жактар үчүн кагаз түрүндөгү квалификацияланган сертификаттын жалпы түрү

1. Квалификацияланган сертификаттын номери: <serialNumber> Квалификацияланган сертификаттын жарактуу мөөнөтү: <validity.notBefore> тартып <validity.notAfter> чейин

2. Квалификацияланган сертификат ээси тууралуу маалымат

- толук аты-жөнү: <commonName>

- ПИН <PIN >

3. Квалификацияланган сертификаттын басып чыгаруучусу маалымат

- күбөлөндүрүүчү борбордун аталышы: <commonName>

- күбөлөндүрүүчү борбордун жайгашкан жери: <countryName>, <stateOrProvinceName>, <localityName>, <streetAddress>

- * күбөлөндүрүүчү борбордун ишенимдүү жагы: <title><surname><givenName>

4. Күбөлөндүрүүчү борбордун квалификацияланган сертификатынын номери: <authorityKeyIdentifier.authorityCertSerialNumber>

5. Электрондук колтамга каражатынын аталышы: <issuerSignTool.signTool>

6. Электрондук колтамга каражатынын шайкештигин тастыктоо тууралуу корутундунун реквизиттери: <issuerSignTool.sign ToolCert>

7. Күбөлөндүрүүчү борбордун каражатынын аталышы: <issuerSignTool.cATool>

8. Күбөлөндүрүүчү борбордун каражатынын шайкештигин тастыктоо тууралуу корутундунун реквизиттери: <issuerSignTool.cAToolCert>

9. Электрондук колтамга текшерүү ачкычы тууралуу маалымат

- колдонулган алгоритм: <algorithm>
- * колдонулган электрондук колтамга каражаты: <subjectSignTool>
- ачкычты колдонуу жааты: <keyUsage>
- ачкычтын мааниси: subjectPublicKey>

10. Квалификацияланган сертификат боюнча электрондук колтамга

- колдонулган алгоритм: <algorithmIdentifier>
- электрондук колтамганын мааниси: <encrypted>

Ыйгарым укуктуу адамдын кол тамгасы___________ /<колтамганын чечмелениши>/

“*” белгиси менен белгиленген талаалар квалификацияланган сертификатта жок болушу мүмкүн.

5-глава. Юридикалык жактар үчүн кагаз түрүндөгү квалификацияланган сертификаттын жалпы түрү

1. Квалификацияланган сертификаттын номери: <serialNumber>

2. Квалификацияланган сертификаттын жарактуу мөөнөтү: <validity.notBefore> тартып <validity.notAfter> чейин

3. Квалификацияланган сертификат ээси тууралуу маалымат

- юридикалык жактын аталышы <commonName>
- ИНН: <INN>
- Юридикалык жактын жайгашкан жери: <countryName>, <stateOrProvinceName>, <localityName>, <streetAddress>,
- * Юридикалык жактын ыйгарым укуктуу өкүлү:

____

4. Квалификацияланган сертификаттын басып чыгаруучусу тууралуу маалымат

- Күбөлөндүрүүчү борбордун аталышы: <commonName>
- Күбөлөндүрүүчү борбордун жайгашкан жери: <countryName>, <stateOrProvinceName>, <localityName>, <streetAddress>

* Күбөлөндүрүүчү борбордун ишенимдүү жагы: <title><surname><givenName>

5. Күбөлөндүрүүчү борбордун квалификацияланган сертификатынын номери: <authorityKeyIdentifier.authorityCertSerialNumber>

6. Электрондук колтамга каражатынын аталышы: <issuerSignTool.signTool>

7. Электрондук колтамга каражатынын шайкештигин тастыктоо тууралуу корутундунун реквизиттери: <issuerSignTool.signToolCert>

8. Күбөлөндүрүүчү борбордун каражатынын аталышы: <issuerSignTool.cATool>

9. Күбөлөндүрүүчү борбордун каражатынын шайкештигин тастыктоо тууралуу корутундунун реквизиттери: <issuerSignTool.cAToolCert>

10. Электрондук колтамга текшерүү ачкычы тууралуу маалымат

- Колдонулган алгоритм: <algorithm>
- * Колдонулган электрондук колтамга каражат: <subjectSignTool>

Ачкычты колдонуу жааты: <keyUsage>

- Ачкычтын маани: <subjectPublicKey>

11. Квалификацияланган сертификат боюнча электрондук колтамга

- колдонулган алгоритм: <algorithmIdentifier>
- электрондук колтамганын мааниси: <encrypted>

Ыйгарым укуктуу адамдын кол тамгасы___________ /<колтамганын чечмелениши>/

“*” белгиси менен белгиленген талаалар квалификацияланган сертификатта жок болушу мүмкүн.

6-глава. Ушул талаптарда колдонулган стандарттардын тизмеси

1. Ачык системалардагы аутентификациянын негиздери “Маалымат технологиясы. Ачык системалардын өз ара байланышы. Маалымдама. 8-бөлүк. Аутентификациянын негиздери” Р МСТ СЭАУ/ЭАЭТК 9594-8-98 аныкталган.

2. Ачык ачкыч сертификатынын жана атрибут сертификатынын түзүмү ISO/IEC 9594-8:2020 “Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks” эл аралык стандартта аныкталып, http://www.itu.int/rec/T-REC-X.509-201910-I/en Интернеттин маалымат-телекоммуникациялык тармагына жарыяланган.

3. Сертификаттын жана жокко чыгарылган сертификат тизмесинин профили IETF RFC 5280 (2008) “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” сунуштамаларында аныкталып, Интернеттин маалымат-телекоммуникациялык тармагына жарыяланган: http://www.ietf.org/rfc/rfc5280.txt.

4. 1-версиянын абстракттуу синтаксистик нотациясынын спецификациясы “Маалымат технологиясы. 1-версиянын абстракттуу синтаксистик нотациясы (АСН.1). 1-бөлүк. Негизги нотациянын спецификациясы” Р МСТ СЭАУ/ЭАЭТК 8824-1-2001 аныкталган. (ISO/IEC 8824-1:2001 Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation).

5. Тандалган атрибуттардын түрлөрү “Маалымат технологиясы. Ачык тутумдардын өз ара байланышы. Маалымдама. 6-бөлүк. Атрибуттардын

тандалган түрлөрү” Р МСТ СЭАУ/ЭАЭТК 9594-6-98 жана “Information technology – Open systems interconnection – The Directory: Selected attribute types” ISO/IEC 9594-6:2019 эл аралык стандартта аныкталган, Интернеттин маалымат-телекоммуникациялык тармагына жарыяланган: http://www.itu.int/rec/T-REC-X.509-201910-I/en.

6. Эки белгиден турган өлкөнүн коддору “Маалымат, китепкана жана басып чыгаруу иши боюнча стандарттар тутуму. Өлкө аталыштарынын коддору” МСТ 7.67-2024 аныкталган.