Приложение 1

ТРЕБОВАНИЯ
к форме квалифицированного сертификата электронной подписи

Глава 1. Общие положения

1. Настоящие Требования к форме квалифицированного сертификата электронной подписи (далее – Требования) предназначены для определения условий по формированию квалифицированных сертификатов ключей проверки подписи аккредитованными удостоверяющими центрами.

2. Настоящие Требования разработаны в соответствии с Законом Кыргызской Республики «Об электронной подписи» (далее – Закон) и во исполнение пункта 2 постановления Правительства Кыргызской Республики «О некоторых вопросах, связанных с использованием электронной подписи» от 31 декабря 2019 года № 742.

3. Настоящие Требования не распространяются на средства защиты сведений, относящиеся к государственным секретам Кыргызской Республики.

4. В настоящих Требованиях используются следующие понятия в соответствии с Законом:

1) электронная подпись (далее – ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме и (или) логически связана с ней и которая используется для определения лица, от имени которого подписана информация;

2) сертификат ключа проверки подписи – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром и подтверждающий принадлежность ключа проверки подписи владельцу сертификата ключа проверки подписи;

3) квалифицированный сертификат ключа проверки подписи (далее – квалифицированный сертификат) – сертификат ключа проверки подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо органом исполнительной власти, уполномоченным в сфере использования ЭП, осуществляющим функции главного (корневого) удостоверяющего центра;

4) владелец сертификата ключа проверки подписи – лицо, которому в порядке, установленном Законом, удостоверяющим центром выдан сертификат ключа проверки подписи;

5) ключ подписи – уникальная последовательность символов, предназначенная для создания ЭП;

6) ключ проверки подписи – уникальная последовательность символов, однозначно связанная с ключом подписи и предназначенная для проверки подлинности ЭП (далее – проверка ЭП);

7) удостоверяющий центр (далее - УЦ) – юридическое лицо или индивидуальный предприниматель, осуществляющие деятельность по созданию и выдаче сертификатов ключа проверки подписи;

8) аккредитация УЦ – признание органом исполнительной власти, уполномоченным в сфере использования ЭП, соответствия УЦ требованиям, установленным Законом;

9) средства ЭП – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание ЭП, проверка ЭП, создание ключей подписи и ключей проверки подписи;

10) средства УЦ – программные и (или) аппаратные средства, используемые для реализации функций создания, хранения и выдачи сертификатов ключа проверки подписи, а также ведения реестра сертификатов ключа проверки подписи;

Глава 2. Требования к форме квалифицированного сертификата

5. Настоящие Требования определяют обязательные и дополнительные поля квалифицированного сертификата (далее – форма квалифицированного сертификата).

6. Назначение дополнительных полей квалифицированного сертификата и их расположение в квалифицированном сертификате определяются в техническом задании на разработку (модернизацию) средств УЦ.

7. В соответствии с Законом квалифицированный сертификат должен содержать следующую информацию:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
- фамилию, имя и отчество (если имеется), дату и место рождения владельца квалифицированного сертификата - физического лица либо наименование (фирменное наименование), регистрационный номер, место регистрации и (или) место фактического нахождения исполнительного органа владельца квалифицированного сертификата – юридического лица;
- идентификационный номер налогоплательщика (далее – ИНН) владельца квалифицированного сертификата – для юридического лица или персональный идентификационный номер налогоплательщика (далее – ПИН) владельца квалифицированного сертификата – для физического лица;
- ключ проверки подписи;
- наименование средств ЭП и средств УЦ, которые использованы для создания ключа подписи, ключа проверки подписи и квалифицированного

сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с Законом;

- наименование и местонахождение аккредитованного УЦ, который выдал квалифицированный сертификат, номер квалифицированного сертификата УЦ и реквизиты свидетельства об аккредитации этого центра;

- ограничения использования квалифицированного сертификата (если ограничения устанавливаются);

- иные сведения о заявителе (по требованию заявителя).

8. Если заявителем представлены в аккредитованный УЦ документы, подтверждающие его право действовать от имени третьих лиц, в квалифицированный сертификат включаются сведения, свидетельствующие о таких правомочиях заявителя и сроке действия указанных правомочий.

8^1. В случае аннулирования квалифицированного сертификата, выданного аккредитованному УЦ, который выдал квалифицированный сертификат заявителю, а также в случае в аннулирование или истечении срока аккредитации УЦ квалифицированный сертификат, выданный аккредитованным УЦ заявителю, прекращает свое действие.

8^2. Владелец квалифицированного сертификата при наличии основания полагать, что конфиденциальность ключа ЭП нарушена, обязан прекратить использование данного ключа и немедленно обратиться в УЦ, выдавший квалифицированный сертификат, для прекращения действия этого сертификата.

Глава 3. Требования к порядку расположения полей квалифицированного сертификата

9. Требования к порядку расположения полей квалифицированного сертификата устанавливаются в соответствии с основами аутентификации в открытых системах (см. пункт 1 главы 6 Требований), структурой сертификата открытого ключа и сертификата атрибутов (см. пункт 2 главы 6 Требований) и профилем сертификата и списка аннулированных сертификатов (см. пункт 3 главы 6 Требований).

10. Структура квалифицированного сертификата в форме электронного документа, определенная в соответствии со спецификацией абстрактной синтаксической нотации версии один (см. пункт 4 главы 6 Требований), должна иметь следующий общий вид:

```
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. Поле algorithmIdentifier (идентификатор алгоритма) содержит идентификатор криптографического алгоритма, с использованием которого аккредитованный УЦ, доверенное лицо аккредитованного УЦ либо уполномоченный орган сформировал ЭП настоящего квалифицированного сертификата.

Дополнительно могут быть указаны параметры криптографического алгоритма:

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

12. Поле encrypted содержит ЭП, сформированную аккредитованным УЦ, доверенным лицом аккредитованного УЦ либо уполномоченным органом под структурированной совокупностью полей квалифицированного сертификата (toBeSigned).

13. Поле version (версия) содержит номер версии формата сертификата: Version::= INTEGER { v1(0), v2(1), v3(2) }.

14. Ввиду необходимости использования дополнений сертификата значение поля version должно равняться 2.

15. Поле serialNumber (серийный номер) должно содержать положительное целое число, однозначно идентифицирующее квалифицированный сертификат в множестве всех сертификатов, выданных данным аккредитованным УЦ, доверенным лицом аккредитованного УЦ либо уполномоченным органом: CertificateSerialNumber::= INTEGER.

16. Поле signature (подпись) содержит идентификатор криптографического алгоритма, с использованием которого аккредитованный УЦ, доверенное лицо аккредитованного УЦ либо уполномоченный орган сформировали ЭП данного квалифицированного

сертификата. Содержимое данного поля должно совпадать с содержимым поля algorithmIdentifier.

17. Поле issuer (издатель) имеет тип Name и идентифицирует аккредитованный УЦ, доверенное лицо аккредитованного УЦ либо уполномоченный орган, создавшие и выдавшие данный квалифицированный сертификат. Тип Name описывается следующим образом:

```
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.
```

Тип поля value определяется типом атрибута, но в общем случае в качестве AttributeValue выступает тип DirectoryString:

```
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. Стандартные атрибуты имени описаны в справочнике выбранных типов атрибутов (см. пункт 5 главы 6 Требований). При описании формы квалифицированного сертификата используются следующие стандартные атрибуты имени:

1) commonName (ФИО).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую имя, фамилию и отчество (если имеется) - для физического лица или наименование – для юридического лица. Объектный идентификатор типа атрибута commonName имеет вид 2.5.4.3;

2) surname (фамилия).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую фамилию физического лица. Объектный идентификатор типа атрибута surname имеет вид 2.5.4.4;

3) givenName (приобретенное имя).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую имя и отчество (если имеется) физического лица. Объектный идентификатор типа атрибута givenName имеет вид 2.5.4.42;

4) countryName (наименование страны).

В качестве значения данного атрибута имени следует использовать двухсимвольный код страны (см. пункт 6 главы 6 Требований). Объектный идентификатор типа атрибута countryName имеет вид 2.5.4.6;

5) stateOrProvinceName (наименование области).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование соответствующей области Кыргызской Республики. Объектный идентификатор типа атрибута stateOrProvinceName имеет вид 2.5.4.8;

6) localityName (наименование населенного пункта).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование соответствующего населенного пункта. Объектный идентификатор типа атрибута localityName имеет вид 2.5.4.7;

7) streetAddress (название улицы, номер дома).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую часть адреса места нахождения соответствующего лица, включающую наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется). Объектный идентификатор типа атрибута streetAddress имеет вид 2.5.4.9;

8) organizationName (наименование организации).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование юридического лица. Объектный идентификатор типа атрибута organizationName имеет вид 2.5.4.10;

9) organizationUnitName (подразделение организации).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование подразделения юридического лица. Объектный идентификатор типа атрибута organizationUnitName имеет вид 2.5.4.11;

10) title (должность).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование должности лица. Объектный идентификатор типа атрибута title имеет вид 2.5.4.12.

Для включения в квалифицированный сертификат иной информации о владельце квалифицированного сертификата рекомендуется использовать стандартные атрибуты имени, описанные в справочнике выбранных типов атрибутов.

19. К дополнительным атрибутам имени относятся:

1) INN (ИНН ЮЛ)

В качестве значения данного атрибута имени следует использовать текстовую строку, состоящую из 14 цифр и представляющую идентификационный номер налогоплательщика юридического лица квалифицированного сертификата. Объектный идентификатор типа атрибута INNLE имеет вид 1.2.643.100.4, тип атрибута INN LE описывается следующим образом: INNLE::= NUMERIC STRING SIZE 14;

2) PIN (ПИН ФЛ)

В качестве значения данного атрибута имени следует использовать текстовую строку, состоящую из 14 цифр и представляющую персональный идентификационный номер владельца квалифицированного сертификата. Объектный идентификатор типа атрибута INN имеет вид 1.2.643.3.131.1.1, тип атрибута INN описывается следующим образом: INN::= NUMERIC STRING SIZE 14;

3) dateOfBirth (дата рождения).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую дату рождения физического лица в формате «DD.MM.YYYY». Объектный идентификатор типа атрибута dateOfBirth имеет вид 1.3.6.1.5.5.7.9.1;

4) placeOfBirth (место рождения).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую место рождения физического лица. Объектный идентификатор типа атрибута placeOfBirth имеет вид 1.3.6.1.5.5.7.9.2;

5) description (описание).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую реквизиты свидетельства об аккредитации УЦ. Объектный идентификатор типа атрибута description имеет вид 2.5.4.13.

20. Поле validity имеет тип Validity и содержит даты начала и окончания действия квалифицированного сертификата. Тип Validity описывается следующим образом:

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

21. Поле subject имеет тип Name и идентифицирует владельца квалифицированного сертификата.

22. Поле subjectPublicKeyInfo имеет тип SubjectPublicKeyInfo и содержит значение ключа проверки ЭП владельца квалифицированного сертификата, а также идентификатор криптографического алгоритма, с которым должен использоваться данный ключ:

```
SubjectPublicKeyInfo::=SEQUENCE{algorithm
AlgorithmIdentifier, subjectPublicKey BIT STRING }.
```

23. Необязательные поля issuerUniqueIdentifier и subjectUniqueIdentifier имеют тип UniqueIdentifier. Настоящие Требования не устанавливают требований к использованию указанных полей.

24. Дополнительная информация, касающаяся использования квалифицированного сертификата, включается в состав дополнений:

```
Extensions::= SEQUENCE {
```

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

Для включения в квалифицированный сертификат иной информации о владельце квалифицированного сертификата, для которой не предусмотрены соответствующие стандартные атрибуты имени, в том числе информации о правомочиях владельца квалифицированного сертификата и сроке их действия, рекомендуется использовать дополнение subjectAlternativeName.

25. Дополнение authorityKeyIdentifier (идентификатор ключа УЦ) имеет тип AuthorityKeyIdentifier, структура которого определяется следующим образом:

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

В квалифицированном сертификате следует использовать дополнение authorityKeyIdentifier с занесением в поле authorityCertSerialNumber номера соответствующего квалифицированного сертификата аккредитованного УЦ или доверенного лица аккредитованного УЦ либо уполномоченного органа, создавшего исходный квалифицированный сертификат. Объектный идентификатор типа дополнения authorityKeyIdentifier имеет вид 2.5.29.35.

26. Дополнение keyUsage определяет область использования ключа проверки ЭП, содержащегося в поле subjectPublicKeyInfo квалифицированного сертификата. Дополнение keyUsage имеет тип KeyUsage, структура которого определяется следующим образом:

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

Значение «1» в нулевом бите означает, что область использования ключа включает проверку ЭП под электронными документами, отличными от квалифицированных сертификатов и списков уникальных номеров квалифицированных сертификатов ключей проверки ЭП, действие которых на определенный момент было прекращено УЦ до истечения их действия

(далее – список аннулированных сертификатов), предназначенными для выполнения процедур аутентификации или контроля целостности.

Значение «1» в первом бите означает, что область использования ключа включает проверку ЭП под электронными документами, отличными от квалифицированных сертификатов и списков аннулированных сертификатов, в отношении которых ставится задача обеспечения невозможности отказа подписавшего лица от своего действия.

Значение «1» во втором бите означает, что область использования ключа включает зашифрование закрытых или секретных ключей, например, в целях их защищенной доставки.

Значение «1» в третьем бите означает, что область использования ключа включает непосредственно зашифрование пользовательских данных без дополнительного использования методов симметричной криптографии.

Значение «1» в четвертом бите означает, что область использования ключа включает согласование ключей.

Значение «1» в пятом бите означает, что область использования ключа включает проверку подписей под квалифицированными сертификатами.

Значение «1» в шестом бите означает, что область использования ключа включает проверку подписей под списками аннулированных сертификатов.

Значение «1» в седьмом бите означает, что область использования ключа включает зашифрование данных в процессе согласования ключей (при этом в четвертом бите должно быть значение «1»).

Значение «1» в восьмом бите означает, что область использования ключа включает расшифрование данных в процессе согласования ключей (при этом в четвертом бите должно быть значение «1»).

Объектный идентификатор дополнения keyUsage имеет вид 2.5.29.15.

27. Дополнение certificatePolicies предназначено для обозначения политик сертификации, в соответствии с которыми должен использоваться квалифицированный сертификат. Тип CertificatePoliciesSyntax, описывающий дополнение certificatePolicies, определяется следующим образом:

```
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.
```

Объектный идентификатор дополнения certificatePolicies имеет вид 2.5.29.32.

28. Для указания в квалифицированном сертификате наименования используемого владельцем квалифицированного сертификата средства ЭП должно использоваться некритичное дополнение subjectSignTool типа UTF8String SIZE(1..200), объектный идентификатор которого имеет вид 1.2.643.100.111.

29. Для указания в квалифицированном сертификате наименования средств ЭП и средств аккредитованного УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, квалифицированного сертификата, а также реквизитов документа, подтверждающего соответствие указанных средств требованиям, установленным законодательством Кыргызской Республики, должно использоваться некритичное дополнение issuerSignTool типа IssuerSignTool, имеющего следующее представление:

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

В строковом поле signTool должно содержаться полное наименование средства ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП и квалифицированного сертификата.

В строковом поле cATool должно содержаться полное наименование средства аккредитованного УЦ, которое было использовано для создания ключа ЭП, ключа проверки ЭП и квалифицированного сертификата.

В строковом поле signToolCert должны содержаться реквизиты заключения о подтверждении соответствия средства ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП, требованиям, установленным в соответствии с Законом (далее – заключение о подтверждении соответствия средства ЭП).

В строковом поле cAToolCert должны содержаться реквизиты заключения о подтверждении соответствия средства УЦ, которое было использовано для создания квалифицированного сертификата, требованиям, установленным в соответствии с Законом (далее – заключение о подтверждении соответствия средства УЦ).

Объектный идентификатор типа IssuerSignTool имеет вид 1.2.643.100.112.

30. Форма квалифицированного сертификата на бумажном носителе должна удовлетворять следующим требованиям:

- отображение полей квалифицированного сертификата в виде, пригодном для восприятия человеком;

- отображение содержащейся в квалифицированном сертификате информации на государственном и официальном языках на кириллице;

- обеспечивать пригодность для проведения формализованной процедуры контроля соответствия квалифицированного сертификата в формах электронного документа и документа на бумажном носителе.

Допускается не отображать в квалифицированном сертификате на бумажном носителе значения полей, которые фиксированы для всех квалифицированных сертификатов (например, поле version имеет значение 2, соответствующее версии v3).

Допускается в квалифицированном сертификате на бумажном носителе однократно отображать информацию, которая дублируется в различных полях (например, algorithmIdentifier и signature).

Общий вид квалифицированного сертификата на бумажном носителе для физических лиц приведен в главе 4 настоящих Требований.

Общий вид квалифицированного сертификата на бумажном носителе для юридических лиц приведен в главе 5 настоящих Требований.

Глава 4. Общий вид квалифицированного сертификата на бумажном носителе для физических лиц

1. Номер квалифицированного сертификата: <serialNumber>
Действие квалифицированного сертификата: с <validity.notBefore> по <validity.not After>

2. Сведения о владельце квалифицированного сертификата

- Фамилия, имя, отчество: <commonName>
- ПИН <PIN >

3. Сведения об издателе квалифицированного сертификата

- Наименование УЦ: <commonName>
- Место нахождения УЦ: <countryName>, <stateOrProvinceName>, <localityName>, <streetAddress>
-* Доверенное лицо УЦ: <title><surname><givenName>

4. Номер квалифицированного сертификата УЦ: <authorityKeyIdentifier.authorityCertSerialNumber>

5. Наименование средства ЭП: <issuerSignTool.signTool>

6. Реквизиты заключения о подтверждении соответствия средства ЭП: <issuerSignTool.signToolCert>

7. Наименование средства УЦ: <issuerSignTool.cATool>

8. Реквизиты заключения о подтверждении соответствия средства УЦ: <issuerSignTool.cAToolCert>

9. Сведения о ключе проверки ЭП

- Используемый алгоритм: <algorithm>
- * Используемое средство ЭП: <subjectSignTool>
-Область использования ключа: <keyUsage>
- Значение ключа: <subjectPublicKey>

10. ЭП под квалифицированным сертификатом

- Используемый алгоритм: <algorithmIdentifier>

- Значение ЭП: <encrypted>

Подпись уполномоченного лица _____ /<расшифровка подписи>/

Символом «*» отмечены поля, которые в квалифицированном сертификате могут отсутствовать.

Глава 5. Общий вид квалифицированного сертификата на бумажном носителе для юридических лиц

1. Номер квалифицированного сертификата: <serialNumber>
2. Действие квалифицированного сертификата: с <validity.notBefore>по <validity.notAfter>
3. Сведения о владельце квалифицированного сертификата
- Наименование юридического лица <commonName>
- ИНН: <INN>
- Место нахождения юридического лица: <countryName>, <stateOrProvinceName>, <localityName>, <streetAddress>,
- * Уполномоченный представитель юридического лица: _____
4. Сведения об издателе квалифицированного сертификата
- Наименование УЦ: <commonName>
- Место нахождения УЦ: <countryName>, <stateOrProvinceName>, <localityName>, <streetAddress>
- * Доверенное лицо УЦ: <title><surname><givenName>
5. Номер квалифицированного сертификата УЦ: <authorityKeyIdentifier.authorityCertSerialNumber>
6. Наименование средства ЭП: <issuerSignTool.signTool>
7. Реквизиты заключения о подтверждении соответствия средства ЭП: <issuerSignTool.signToolCert>
8. Наименование средства УЦ: <issuerSignTool.cATool>
9. Реквизиты заключения о подтверждении соответствия средства УЦ: <issuerSignTool.cAToolCert>
10. Сведения о ключе проверки ЭП
- Используемый алгоритм: <algorithm>
- * Используемое средство ЭП: <subjectSignTool>
Область использования ключа: <keyUsage>
- Значение ключа: <subjectPublicKey>
11. ЭП под квалифицированным сертификатом
- Используемый алгоритм: <algorithmIdentifier>
- Значение ЭП: <encrypted>

Подпись уполномоченного лица _____ /<расшифровка подписи>/

Символом «*» отмечены поля, которые в квалифицированном сертификате могут отсутствовать.

Глава 6. Перечень стандартов, используемых в настоящих требованиях

1. Основы аутентификации в открытых системах определены в ГОСТ Р ИСО/МЭК 9594-8-98 «Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации».

2. Структура сертификата открытого ключа и сертификата атрибутов определена в международном стандарте ISO/IEC 9594-8:2020 «Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks», опубликованном по адресу в информационно-телекоммуникационной сети Интернет: http://www.itu.int/rec/T-REC-X.509-201910-I/en.

3. Профиль сертификата и списка аннулированных сертификатов определен в рекомендациях IETF RFC 5280 (2008) «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», опубликованных по адресу в информационно-телекоммуникационной сети Интернет: http://www.ietf.org/rfc/rfc5280.txt.

4. Спецификация абстрактной синтаксической нотации версии один определена в ГОСТ Р ИСО/МЭК 8824-1-2001 «Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 1. Спецификация основной нотации». (ISO/IEC 8824-1:2001 Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation)

5. Выбранные типы атрибутов определены в ГОСТ Р ИСО/МЭК 9594-6-98 «Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 6. Выбранные типы атрибутов» и в международном стандарте ISO/IEC 9594-6:2019 «Information technology - Open systems interconnection - The Directory: Selected attribute types», опубликованном по адресу в информационно-телекоммуникационной сети Интернет: http://www.itu.int/rec/T-REC-X.509-201910-I/en.

6. Двухсимвольные коды стран определены в ГОСТ 7.67-2024 «Система стандартов по информации, библиотечному и издательскому делу. Коды названий стран».