МИНИСТЕРСТВО ГОСУДАРСТВЕННОЙ БЕЗОПАСНОСТИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ

ПРИКАЗ

«27» мая 2020 года г. Донецк № 83

МИНИСТЕРСТВО ЮСТИЦИИ
ДОНЕЦКОЙ НАРОДНОЙ
РЕСПУБЛИКИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 3898
от «17» июня 2020 г.

Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи

В соответствии с пунктом 36 части 1 статьи 16 Закона Донецкой Народной Республики «О Министерстве государственной безопасности», пунктом 1 части 5 статьи 8 Закона Донецкой Народной Республики «Об электронной подписи»

ПРИКАЗЫВАЮ:

1. Утвердить Требования к форме квалифицированного сертификата ключа проверки электронной подписи (прилагаются).

2. Направить настоящий Приказ на государственную регистрацию в Министерство юстиции Донецкой Народной Республики.

3. Контроль исполнения настоящего Приказа возложить на Министерство государственной безопасности Донецкой Народной Республики.

4. Настоящий Приказ вступает в силу со дня его официального опубликования.

Министр В.Н. Павленко

УТВЕРЖДЕНЫ

Приказом Министерства
государственной безопасности
Донецкой Народной Республики
от 27 05 2020 г. № 83

Требования к форме квалифицированного сертификата ключа проверки электронной подписи

I. Общие положения

1.1. Настоящие Требования разработаны в соответствии с Законом Донецкой Народной Республики «Об электронной подписи» (далее – Закон).

1.2. В настоящих Требованиях используются понятия, определенные в статье 2 Закона.

1.3. Настоящие Требования устанавливают требования к совокупности и порядку расположения полей квалифицированного сертификата (далее – форма квалифицированного сертификата).

1.4. При включении в состав квалифицированного сертификата дополнительных полей требования к их назначению и расположению в квалифицированном сертификате определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

II. Требования к совокупности полей квалифицированного сертификата

2.1. Требования к совокупности полей квалифицированного сертификата устанавливаются на основании Закона.

2.2. В соответствии со статьями 14 и 17 Закона квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат) должен содержать следующую информацию:

а) уникальный номер квалифицированного сертификата;

б) даты начала и окончания действия квалифицированного сертификата;

в) фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата – для физического лица, либо наименование и место нахождения владельца квалифицированного сертификата – для юридического лица, а также в случаях, предусмотренных Законом, фамилия, имя и отчество физического лица, действующего от имени юридического лица на основании учредительных документов юридического лица или доверенности (далее – уполномоченный представитель юридического лица);

г) индивидуальный код юридического лица (далее – ИКЮЛ) владельца квалифицированного сертификата – для юридического лица;

д) регистрационный номер учетной карточки налогоплательщика (далее – РНУКН) владельца квалифицированного сертификата;

е) ключ проверки электронной подписи;

ж) наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствует ключ электронной подписи и ключ проверки электронной подписи;

з) наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с Законом;

и) наименование и место нахождения аккредитованного удостоверяющего центра, который выдал квалифицированный сертификат;

к) номер квалифицированного сертификата аккредитованного удостоверяющего центра;

л) ограничения использования квалифицированного сертификата (если такие ограничения установлены).

2.3. Квалифицированный сертификат должен содержать квалифицированную электронную подпись аккредитованного удостоверяющего центра, подтверждающую принадлежность ключа проверки электронной подписи владельцу квалифицированного сертификата.

2.4. По требованию лица, обратившегося за получением квалифицированного сертификата (далее – заявитель), в квалифицированный сертификат может дополнительно включаться иная информация о владельце квалифицированного сертификата.

Если заявителем представлены в аккредитованный удостоверяющий центр документы, подтверждающие его право действовать от имени третьих лиц, в квалифицированный сертификат может быть включена информация о таких правомочиях заявителя и сроке их действия.

III. Требования к порядку расположения полей квалифицированного сертификата

3.1. Требования к порядку расположения полей квалифицированного сертификата устанавливаются в соответствии с основами аутентификации в открытых системах (Основы аутентификации в открытых системах определены в ГОСТ Р ИСО/МЭК 9594-8-98 "Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации"), структурой сертификата открытого ключа и сертификата атрибутов (Структура сертификата открытого ключа и сертификата атрибутов определена в международном стандарте ISO/IEC 9594-8:2008 "Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks") и профилем сертификата и списка аннулированных сертификатов (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").

3.2. Структура квалифицированного сертификата в форме электронного документа, определенная в соответствии со спецификацией абстрактной синтаксической нотации версии один (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"), 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 } ).
```

3.3. Поле algorithmIdentifier (идентификатор алгоритма) содержит идентификатор криптографического алгоритма, с использованием которого аккредитованный удостоверяющий центр сформировал электронную подпись настоящего квалифицированного сертификата. Дополнительно могут быть указаны параметры криптографического алгоритма:

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

3.4. Поле encrypted содержит электронную подпись, сформированную аккредитованным удостоверяющим центром под структурированной совокупностью полей квалифицированного сертификата (toBeSigned).

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

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

3.6. Поле serialNumber (серийный номер) должно содержать положительное целое число, однозначно идентифицирующее квалифицированный сертификат в множестве всех сертификатов, выданных данным аккредитованным удостоверяющим центром:

```
CertificateSerialNumber ::= INTEGER.
```

3.7. Поле signature (подпись) содержит идентификатор криптографического алгоритма, с использованием которого аккредитованный удостоверяющий центр сформировал электронную подпись данного квалифицированного сертификата. Содержимое данного поля должно совпадать с содержимым поля algorithmIdentifier.

3.8. Поле issuer (издатель) имеет тип Name и идентифицирует аккредитованный удостоверяющий центр, создавший и выдавший 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)) }.
```

3.9. Стандартные атрибуты имени описаны в справочнике выбранных типов атрибутов (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 9594-6:2008 "Information technology – Open systems interconnection – The Directory: Selected attribute types"). При описании формы квалифицированного сертификата используются следующие стандартные атрибуты имени:

а) commonName (общее имя);

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

б) 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;

в) 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;

г) countryName (наименование страны);

в качестве значения данного атрибута имени следует использовать двухсимвольный код страны согласно ГОСТ 7.67-2003 (ИСО 3166-1:1997) «Система стандартов по информации, библиотечному и издательскому делу. Коды названий стран». Объектный идентификатор типа атрибута countryName имеет вид 2.5.4.6;

д) stateOrProvinceName (наименование штата, области или района);

в качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование соответствующего района Донецкой Народной Республики. Объектный идентификатор типа атрибута stateOrProvinceName имеет вид 2.5.4.8;

е) 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;

ж) 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;

з) 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;

и) 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;

к) 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.

3.10. К дополнительным атрибутам имени, необходимость использования которых устанавливается в соответствии с Законом, относятся:

а) OGRN (ИКЮЛ);

значением атрибута OGRN является строка, состоящая из 8 цифр и представляющая ИКЮЛ владельца квалифицированного сертификата – юридического лица. Объектный идентификатор типа атрибута OGRN имеет вид 1.2.643.100.1, тип атрибута OGRN описывается следующим образом:

OGRN ::= NUMERIC STRING SIZE 8;

б) INN (РНУКН);

значением атрибута INN является строка, состоящая из 10 цифр и представляющая РНУКН 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 10.

3.11. 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 }.
```

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

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

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

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

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

```
Extensions ::= SEQUENCE {
        extnId         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.

3.16. Дополнение authorityKeyIdentifier (идентификатор ключа удостоверяющего центра) 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 удостоверяющего центра или уполномоченного республиканского органа, создавшего исходный квалифицированный сертификат. Объектный идентификатор типа дополнения authorityKeyIdentifier имеет вид 2.5.29.35.

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

```
KeyUsage ::= BIT STRING {
    digitalSignature      (0),
    contentCommitment     (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 электронной подписи под электронными документами, отличными от квалифицированных сертификатов и списков уникальных номеров квалифицированных сертификатов ключей проверки электронной подписи, действие которых на определенный момент было прекращено удостоверяющим центром 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 электронной подписи 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.

3.18. 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 PolicyInformation

PolicyInformation ::= SEQUENCE {
        policyIdentifier        CertPolicyId,
        policyQualifiers        SEQUENCE SIZE (1..MAX) OF
        PolicyQualifierInfo     OPTIONAL }

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
        policyQualifierId       PolicyQualifierId,
        qualifier               ANY DEFINED BY policyQualifierId }

PolicyQualifierId ::= OBJECT IDENTIFIER.
```

Объектный идентификатор дополнения certificatePolicies имеет вид 2.5.29.32.

3.19. Для обозначения класса средств электронной подписи владельца квалифицированного сертификата должны применяться следующие идентификаторы:

а) 1.2.643.100.113.1 – класс средства электронной подписи КС1;

б) 1.2.643.100.113.2 – класс средства электронной подписи КС2;

в) 1.2.643.100.113.3 – класс средства электронной подписи КС3;

г) 1.2.643.100.113.4 – класс средства электронной подписи КВ1;

д) 1.2.643.100.113.5 – класс средства электронной подписи КВ2;

е) 1.2.643.100.113.6 – класс средства электронной подписи КА1.

3.20. Сведения о классе средств электронной подписи владельца квалифицированного сертификата должны быть указаны в дополнении certificatePolicies путем включения следующих идентификаторов:

а) для класса средств электронной подписи КС1: 1.2.643.100.113.1;

б) для класса средств электронной подписи КС2: 1.2.643.100.113.1, 1.2.643.100.113.2;

в) для класса средств электронной подписи КС3: 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643.100.113.3;

г) для класса средств электронной подписи КВ1: 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643.100.113.3, 1.2.643.100.113.4;

д) для класса средств электронной подписи КВ2: 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643.100.113.3, 1.2.643.100.113.4, 1.2.643.100.113.5;

е) для класса средств электронной подписи КА1: 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643. 100.113.3, 1.2.643.100.113.4, 1.2.643.100.113.5, 1.2.643.100.113.6.

Для средств электронной подписи, класс которых отличается от класса средств удостоверяющего центра, в которых используются указанные средства электронной подписи, следует указывать идентификаторы для класса средств

электронной подписи, соответствующего классу средств удостоверяющего центра.

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

3.22. Для указания в квалифицированном сертификате наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизитов документа, подтверждающего соответствие указанных средств требованиям, установленным законодательством Донецкой Народной Республики, должно использоваться некритичное дополнение issuerSignTool типа IssuerSignTool, имеющего следующее представление:

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

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

В строковом поле cATool должно содержаться полное наименование средства аккредитованного удостоверяющего центра, которое было использовано для создания ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата.

В строковом поле signToolCert должны содержаться реквизиты заключения республиканского органа исполнительной власти, реализующего государственную политику в сфере государственной безопасности, о подтверждении соответствия средства электронной подписи, которое было использовано для создания ключа электронной подписи, ключа проверки электронной подписи, требованиям, установленным в соответствии с Законом (далее – заключение о подтверждении соответствия средства электронной подписи).

В строковом поле cAToolCert должны содержаться реквизиты заключения республиканского органа исполнительной власти, реализующего

государственную политику в сфере государственной безопасности, о подтверждении соответствия средства удостоверяющего центра, которое было использовано для создания квалифицированного сертификата, требованиям, установленным в соответствии с Законом (далее – заключение о подтверждении соответствия средства удостоверяющего центра).

Объектный идентификатор типа IssuerSignTool имеет вид 1.2.643.100.112.

IV. Требования к форме квалифицированного сертификата на бумажном носителе

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

а) отображение всех полей квалифицированного сертификата в виде, пригодном для восприятия человеком;

б) отображение содержащейся в квалифицированном сертификате информации о наименованиях, именах, месте нахождения, области применения и другой информации на русском языке с использованием символов кириллического алфавита;

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

4.2. Общий вид квалифицированного сертификата на бумажном носителе для владельца – физического лица приведен в приложении № 1 к настоящим Требованиям.

Общий вид квалифицированного сертификата на бумажном носителе для владельца – юридического лица приведен в приложении № 2 к настоящим Требованиям.

Министр В.Н. Павленко

Приложение 1
к Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи (пункт 4.2)

Общий вид квалифицированного сертификата на бумажном носителе для владельца – физического лица

Номер квалифицированного сертификата: <serialNumber>
Действие квалифицированного сертификата: с <notBefore> по <notAfter>

Сведения о владельце квалифицированного сертификата

Фамилия, имя, отчество: <commonName>
Регистрационный номер учетной карточки налогоплательщика: <INN>

Сведения об издателе квалифицированного сертификата

Наименование удостоверяющего центра: <commonName>
Место нахождения удостоверяющего центра: <countryName>, <localityName>, <streetAddress>
* Доверенное лицо удостоверяющего центра: <surname>, <givenName>
Номер квалифицированного сертификата удостоверяющего центра: <authorityKeyIdentifier.authorityCertSerialNumber>
Наименование средства электронной подписи: <issuerSignTool.signTool>
Реквизиты заключения о подтверждении соответствия средства электронной подписи: <issuerSignTool.signToolCert>
Наименование средства удостоверяющего центра: <issuerSignTool.cATool>
Реквизиты заключения о подтверждении соответствия средства удостоверяющего центра: <issuerSignTool.cAToolCert>
Класс средств удостоверяющего центра: <certificatePolicies>

Сведения о ключе проверки электронной подписи

Используемый алгоритм: <algorithm>
* Используемое средство электронной подписи: <subjectSignTool>
Класс средства электронной подписи: <certificatePolicies>
Область использования ключа: <keyUsage>
Значение ключа: <subjectPublicKey>

Электронная подпись под квалифицированным сертификатом

Используемый алгоритм: <algorithmIdentifier>
Значение электронной подписи: <encrypted>

Подпись уполномоченного лица _____/ (расшифровка подписи) /
М.П.

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

Приложение 2
к Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи (пункт 4.2)

Общий вид квалифицированного сертификата на бумажном носителе для владельца – юридического лица

Номер квалифицированного сертификата: <serialNumber>
Действие квалифицированного сертификата: с <notBefore> по <notAfter>

Сведения о владельце квалифицированного сертификата

Наименование юридического лица: <commonName>
Индивидуальный код юридического лица: <OGRN>
Место нахождения юридического лица: <countryName>, <stateOrProvinceName>, <localityName>, <streetAddress>
* Уполномоченный представитель юридического лица: <title> <surname> <givenName>

Сведения об издателе квалифицированного сертификата

Наименование удостоверяющего центра: <commonName>
Место нахождения удостоверяющего центра: <countryName>, <localityName>, <streetAddress>
* Доверенное лицо удостоверяющего центра: <surname>, <givenName>
Номер квалифицированного сертификата удостоверяющего центра: <authorityKeyIdentifier.authorityCertSerialNumber>
Наименование средства электронной подписи: <issuerSignTool.signTool>
Реквизиты заключения о подтверждении соответствия средства электронной подписи: <issuerSignTool.signToolCert>
Наименование средства удостоверяющего центра: <issuerSignTool.cATool>
Реквизиты заключения о подтверждении соответствия средства удостоверяющего центра: <issuerSignTool.cAToolCert>
Класс средств удостоверяющего центра: <certificatePolicies>

Сведения о ключе проверки электронной подписи

Используемый алгоритм: <algorithm>
* Используемое средство электронной подписи: <subjectSignTool>
Класс средства электронной подписи: <certificatePolicies>
Область использования ключа: <keyUsage>

Значение ключа: <subjectPublicKey>

Электронная подпись под квалифицированным сертификатом

Используемый алгоритм: <algorithmIdentifier>
Значение электронной подписи: <encrypted>

Подпись уполномоченного лица _____/ (расшифровка подписи) /
М.П.

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