

Зарегистрировано в Минюсте России 27 января 2012 г. N 23041

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 27 декабря 2011 г. N 795

**ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ
К ФОРМЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ
ЭЛЕКТРОННОЙ ПОДПИСИ**

Список изменяющих документов
(в ред. Приказов ФСБ России от 29.01.2021 N 31,
от 02.02.2024 N 50)

В соответствии с [частью 5 статьи 8](#) Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" <1> приказываю

<1> Собрание законодательства Российской Федерации, 2011, N 15, ст. 2036; N 27, ст. 3880.

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

(в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

2. Настоящий приказ действует до 1 сентября 2027 г.

(в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

Директор
А.БОРТНИКОВ

Приложение
к приказу ФСБ России
от 27 декабря 2011 г. N 795

ТРЕБОВАНИЯ К ФОРМЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

Список изменяющих документов
(в ред. Приказов ФСБ России от 29.01.2021 N 31,
от 02.02.2024 N 50)

I. Общие положения

1. Настоящие Требования разработаны в соответствии с Федеральным [законом](#) от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" <1> (далее - Федеральный закон).
(в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

<1> Собрание законодательства Российской Федерации, 2011, N 15, ст. 2036; 2020, N 24, ст. 3755.
(сноска введена [Приказом](#) ФСБ России от 29.01.2021 N 31)

2. В настоящих Требованиях используются следующие основные понятия, определенные в [статье 2](#) Федерального закона:

1) электронная подпись (далее - ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

2) ключ ЭП - уникальная последовательность символов, предназначенная для создания ЭП;

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

4) удостоверяющий центр (далее - УЦ) - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки ЭП, а также иные функции, предусмотренные Федеральным [законом](#);
(в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

5) сертификат ключа проверки ЭП - электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП;

6) квалифицированный сертификат ключа проверки ЭП (далее - квалифицированный сертификат) - сертификат ключа проверки ЭП, соответствующий требованиям, установленным Федеральным [законом](#) и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП (далее - уполномоченный федеральный орган), и являющийся в связи с этим официальным документом;
(пп. 6 в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

7) владелец сертификата ключа проверки ЭП - лицо, которому в установленном Федеральным [законом](#) порядке выдан сертификат ключа проверки ЭП;

8) аккредитация УЦ - признание соответствия УЦ требованиям Федерального [закона](#); (пп. 8 в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

9) средства ЭП - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП;

10) средства УЦ - программные и (или) аппаратные средства, используемые для реализации функций УЦ;

11) участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, индивидуальные предприниматели, а также граждане; (в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

12) заявитель - коммерческая организация, некоммерческая организация, индивидуальный предприниматель, физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любое иное физическое лицо, лица, замещающие государственные должности Российской Федерации или государственные должности субъектов Российской Федерации, должностные лица государственных органов, органов местного самоуправления, работники подведомственных таким органам организаций, нотариусы и уполномоченные на совершение нотариальных действий лица, обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки ЭП в УЦ за получением сертификата ключа проверки ЭП в качестве будущего владельца такого сертификата. (пп. 12 введен [Приказом](#) ФСБ России от 29.01.2021 N 31)

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

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 УЦ.

II. Требования к совокупности полей квалифицированного сертификата

5. Требования к совокупности полей квалифицированного сертификата устанавливаются на основании Федерального [закона](#).

6. В соответствии со [статьями 14 и 17](#) Федерального закона квалифицированный сертификат должен содержать следующую информацию:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
- 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 Федеральным [законом](#), фамилия, имя и отчество (если имеется) физического лица, действующего от имени владельца квалифицированного сертификата - юридического лица на основании учредительных документов юридического лица или доверенности (далее - уполномоченный представитель юридического лица);

- страховой номер индивидуального лицевого счета (далее - СНИЛС) владельца квалифицированного сертификата - для физического лица;

- основной государственный регистрационный номер (далее - ОГРН) владельца квалифицированного сертификата - для российского юридического лица;
(в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

- основной государственный регистрационный номер индивидуального предпринимателя (далее - ОГРНИП) - владельца квалифицированного сертификата - для физического лица, являющегося индивидуальным предпринимателем;
(абзац введен [Приказом](#) ФСБ России от 29.01.2021 N 31)

- идентификационный номер налогоплательщика (далее - ИНН) владельца квалифицированного сертификата - для физического лица, российского юридического лица и, при наличии, для иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации);
(в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

- уникальный ключ проверки ЭП;
(в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

- наименование используемого средства ЭП и (или) стандарты, требованиям которых соответствует ключ ЭП и ключ проверки ЭП;

- наименования средств ЭП и средств аккредитованного УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с Федеральным [законом](#);

- наименование и место нахождения аккредитованного УЦ, который выдал квалифицированный сертификат;

- номер квалифицированного сертификата аккредитованного УЦ;

- идентификатор, однозначно указывающий на то, что идентификация заявителя при выдаче сертификата ключа проверки ЭП проводилась либо при его личном присутствии, либо без его личного присутствия с использованием квалифицированной ЭП при наличии действующего квалифицированного сертификата либо посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие

информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" <1> (далее - единая система идентификации и аутентификации) и единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (далее - единая биометрическая система), в порядке, установленном Федеральным [законом](#) от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" <2>;

(в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

<1> [Постановление](#) Правительства Российской Федерации от 28 ноября 2011 г. N 977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (Собрание законодательства Российской Федерации, 2011, N 49 (ч. V), ст. 7284; 2020, N 34, ст. 5484).

(сноска введена [Приказом](#) ФСБ России от 29.01.2021 N 31)

<2> Собрание законодательства Российской Федерации, 2006, N 31 (ч. I), ст. 3448; 2020, N 24, ст. 3751.

(сноска введена [Приказом](#) ФСБ России от 29.01.2021 N 31)

- срок действия ключа ЭП, соответствующего уникальному ключу проверки ЭП, содержащемуся в данном квалифицированном сертификате.

(абзац введен [Приказом](#) ФСБ России от 02.02.2024 N 50)

7. Квалифицированный сертификат должен содержать квалифицированную ЭП аккредитованного УЦ (уполномоченного федерального органа), подтверждающую принадлежность ключа проверки ЭП владельцу квалифицированного сертификата.

(в ред. [Приказа](#) ФСБ России от 02.02.2024 N 50)

8. Если лицом, обратившимся за получением квалифицированного сертификата (далее - заявитель), представлены в аккредитованный УЦ документы, подтверждающие его право действовать от имени третьих лиц, в квалифицированный сертификат может быть включена информация о таких полномочиях заявителя и сроке их действия.

(п. 8 в ред. [Приказа](#) ФСБ России от 02.02.2024 N 50)

III. Требования к порядку расположения полей квалифицированного сертификата

9. Требования к порядку расположения полей квалифицированного сертификата устанавливаются в соответствии с основами аутентификации в открытых системах <3>, структурой сертификата открытого ключа и сертификата атрибутов <4> и профилем сертификата и списка аннулированных сертификатов <3>.

(в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

<3> Справочно: Основы аутентификации в открытых системах определены в [ГОСТ Р](#)

[ИСО/МЭК 9594-8-98](#) "Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации".

<4> Справочно: 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", опубликованном по адресу в информационно-телекоммуникационной сети Интернет: <http://www.itu.int/rec/T-REC-X.509-200811-I/en>.

КонсультантПлюс: примечание.

Нумерация сносок приведена в соответствии с источником

<3> Справочно: 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>.

10. Структура квалифицированного сертификата в форме электронного документа, определенная в соответствии со спецификацией абстрактной синтаксической нотации версии один <4>, должна иметь следующий общий вид:

<4> Справочно: 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".

```
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 либо уполномоченный федеральный орган сформировал ЭП настоящего квалифицированного сертификата. Дополнительно могут быть указаны параметры криптографического алгоритма:

(в ред. Приказа ФСБ России от 02.02.2024 N 50)

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

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

(в ред. Приказа ФСБ России от 02.02.2024 N 50)

13. 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.

14. Поле `serialNumber` (серийный номер) должно содержать положительное целое число, однозначно идентифицирующее квалифицированный сертификат в множестве всех сертификатов, выданных данным аккредитованным УЦ либо уполномоченным федеральным органом:

(в ред. Приказа ФСБ России от 02.02.2024 N 50)

`CertificateSerialNumber ::= INTEGER.`

15. Поле `signature` (подпись) содержит идентификатор криптографического алгоритма, с использованием которого аккредитованный УЦ либо уполномоченный федеральный орган сформировали ЭП данного квалифицированного сертификата. Содержимое данного поля должно совпадать с содержимым поля `algorithmIdentifier`.

(в ред. Приказа ФСБ России от 02.02.2024 N 50)

16. Поле `issuer` (издатель) имеет тип `Name` и идентифицирует аккредитованный УЦ либо уполномоченный федеральный орган, создавшие и выдавшие данный квалифицированный сертификат. Тип `Name` описывается следующим образом:

(в ред. Приказа ФСБ России от 02.02.2024 N 50)

```
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)) }.
```

17. Стандартные атрибуты имени описаны в справочнике выбранных типов атрибутов <1>.

При описании формы квалифицированного сертификата используются следующие стандартные атрибуты имени:

<1> Справочно: Выбранные типы атрибутов определены в [ГОСТ Р ИСО/МЭК 9594-6-98](http://www.gost.ru/standarts/10000/10000_99/10000_99_98/10000_99_98_98.htm) "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", опубликованном по адресу в информационно-телекоммуникационной сети Интернет: <http://www.itu.int/rec/T-REC-X.520-200811-I/en>.

1) `commonName` (общее имя).

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 <1>. Объектный идентификатор типа атрибута `countryName` имеет вид 2.5.4.6;

<1> Справочно: Двухсимвольные коды стран определены в ГОСТ 7.67-2003 (ИСО 3166-1:1997) "Система стандартов по информации, библиотечному и издательскому делу. Коды названий стран".

5) `stateOrProvinceName` (наименование штата или области).

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую наименование соответствующего субъекта Российской Федерации. 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.

18. К дополнительным атрибутам имени, необходимость использования которых устанавливается в соответствии с Федеральным [законом](#), относятся:

1) `OGRN` (ОГРН).

Значением атрибута `OGRN` является строка, состоящая из 13 цифр и представляющая ОГРН 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 13;`

2) `SNILS` (СНИЛС).

Значением атрибута `SNILS` является строка, состоящая из 11 цифр и представляющая СНИЛС владельца квалифицированного сертификата - физического лица. Объектный идентификатор типа атрибута `SNILS` имеет вид 1.2.643.100.3, тип атрибута `SNILS` описывается следующим образом:
`SNILS ::= NUMERIC STRING SIZE 11;`

3) `INN` (ИНН физического лица).

(в ред. [Приказа](#) ФСБ России от 29.01.2021 N 31)

Значением атрибута `INN` является строка, состоящая из 12 цифр и представляющая ИНН владельца квалифицированного сертификата - физического лица. Объектный идентификатор типа

атрибута INN имеет вид 1.2.643.3.131.1.1, тип атрибута INN описывается следующим образом: INN ::= NUMERIC STRING SIZE 12;
(в ред. Приказа ФСБ России от 29.01.2021 N 31)

4) INNLE (ИНН юридического лица).

Значением атрибута INNLE является строка, состоящая из 10 цифр и представляющая ИНН владельца квалифицированного сертификата - юридического лица. Объектный идентификатор типа атрибута INNLE имеет вид 1.2.643.100.4, тип атрибута INNLE описывается следующим образом:

INNLE ::= NUMERIC STRING SIZE 10;
(пп. 4 введен Приказом ФСБ России от 29.01.2021 N 31)

5) OGRNIP (ОГРНИП).

Значением атрибута OGRNIP является строка, состоящая из 15 цифр и представляющая ОГРНИП владельца квалифицированного сертификата - физического лица, являющегося индивидуальным предпринимателем. Объектный идентификатор типа атрибута OGRNIP имеет вид 1.2.643.100.5, тип атрибута OGRNIP описывается следующим образом:

OGRNIP ::= NUMERIC STRING SIZE 15.
(пп. 5 введен Приказом ФСБ России от 29.01.2021 N 31)

19. 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 }
```

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

21. 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 }.
```

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

23. 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 полномочиях владельца квалифицированного сертификата и сроке их действия, рекомендуется использовать дополнение `subjectAlternativeName`.

24. 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 либо уполномоченного федерального органа, создавшего исходный квалифицированный сертификат. Объектный идентификатор типа дополнения `authorityKeyIdentifier` имеет вид 2.5.29.35.

(в ред. Приказа ФСБ России от 02.02.2024 N 50)

25. 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),  
    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 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.

25(1). Дополнение `privateKeyUsagePeriod` определяет срок действия ключа ЭП, соответствующего уникальному ключу проверки ЭП, содержащемуся в данном квалифицированном сертификате.

Дополнение `privateKeyUsagePeriod` имеет тип `PrivateKeyUsagePeriod`, структура которого определяется следующим образом:

```
PrivateKeyUsagePeriod ::= SEQUENCE {
    notBefore      [0]    GeneralizedTime OPTIONAL,
    notAfter       [1]    GeneralizedTime OPTIONAL}.
```

Объектный идентификатор типа `PrivateKeyUsagePeriod` имеет вид 2.5.29.16.
(п. 25(1) введен [Приказом](#) ФСБ России от 02.02.2024 N 50)

26. 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.

27. Для обозначения класса средств ЭП владельца квалифицированного сертификата должны применяться следующие идентификаторы:

- 1.2.643.100.113.1 - класс средства ЭП КС1,

- 1.2.643.100.113.2 - класс средства ЭП КС2,

- 1.2.643.100.113.3 - класс средства ЭП КС3,
- 1.2.643.100.113.4 - класс средства ЭП КВ1,
- 1.2.643.100.113.5 - класс средства ЭП КВ2,
- 1.2.643.100.113.6 - класс средства ЭП КА1.

28. Сведения о классе средств ЭП владельца квалифицированного сертификата должны быть указаны в дополнении certificatePolicies путем включения следующих идентификаторов:

- для класса средств ЭП КС1: 1.2.643.100.113.1,
- для класса средств ЭП КС2: 1.2.643.100.113.1, 1.2.643.100.113.2,
- для класса средств ЭП КС3: 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643.100.113.3,
- для класса средств ЭП 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,
- для класса средств ЭП 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,
- для класса средств ЭП 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.

Абзац утратил силу с 1 сентября 2024 года. - [Приказ](#) ФСБ России от 02.02.2024 N 50.

28.1. Для указания в квалифицированном сертификате идентификатора, однозначно указывающего на то, что идентификация заявителя при выдаче сертификата ключа проверки ЭП проводилась при его личном присутствии или без его личного присутствия с использованием квалифицированной ЭП при наличии действующего квалифицированного сертификата либо без личного присутствия заявителя - гражданина Российской Федерации с применением информационных технологий путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным [законом](#) от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", должно использоваться некритичное дополнение identificationKind типа IdentificationKind, имеющего следующее представление:

```
IdentificationKind ::= INTEGER { personal(0), remote_cert(1), remote_passport(2), remote_system(3)}.
```

В случае, если идентификация заявителя при выдаче сертификата ключа проверки ЭП проводилась при его личном присутствии, дополнение identificationKind должно иметь значение 0.

В случае, если идентификация заявителя при выдаче сертификата ключа проверки ЭП проводилась без его личного присутствия с использованием квалифицированной ЭП при наличии действующего квалифицированного сертификата, дополнение identificationKind должно иметь

значение 1.

В случае, если идентификация заявителя - гражданина Российской Федерации при выдаче сертификата ключа проверки ЭП проводилась без его личного присутствия с применением информационных технологий путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, дополнение `identificationKind` должно иметь значение 2.

В случае, если идентификация заявителя - гражданина Российской Федерации при выдаче сертификата ключа проверки ЭП проводилась без его личного присутствия с применением информационных технологий путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным [законом](#) от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", дополнение `identificationKind` должно иметь значение 3.

Объектный идентификатор типа `IdentificationKind` имеет вид 1.2.643.100.114.
(п. 28.1 введен [Приказом](#) ФСБ России от 29.01.2021 N 31)

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

30. 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 Российской Федерации, должно использоваться не критичное 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 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 ФСБ России о подтверждении соответствия средства ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП, требованиям, установленным в соответствии с Федеральным [законом](#) (далее - заключение о подтверждении соответствия средства электронной подписи).

В строковом поле `cAToolCert` должны содержаться реквизиты заключения ФСБ России о подтверждении соответствия средства УЦ, которое было использовано для создания

квалифицированного сертификата, требованиям, установленным в соответствии с Федеральным [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

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

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

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

- 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).

32. Общий вид квалифицированного сертификата на бумажном носителе для владельца - физического лица приведен в [приложении N 1](#) к настоящим Требованиям.

Общий вид квалифицированного сертификата на бумажном носителе для владельца - юридического лица приведен в [приложении N 2](#) к настоящим Требованиям.

Общий вид квалифицированного сертификата на бумажном носителе для владельца - физического лица, являющегося индивидуальным предпринимателем, приведен в [приложении N 3](#) к настоящим Требованиям.

(абзац введен [Приказом](#) ФСБ России от 29.01.2021 N 31)

Общий вид квалифицированного сертификата на бумажном носителе для владельца - лица, замещающего государственные должности Российской Федерации, государственные должности субъектов Российской Федерации, должностного лица государственных органов, органов местного самоуправления, их подведомственных учреждений, Центрального банка Российской Федерации приведен в [приложении N 4](#) к настоящим Требованиям.

(абзац введен [Приказом](#) ФСБ России от 02.02.2024 N 50)

Общий вид квалифицированного сертификата на бумажном носителе для владельца - филиала (представительства) иностранного юридического лица приведен в [приложении N 5](#) к настоящим Требованиям.

(абзац введен [Приказом](#) ФСБ России от 02.02.2024 N 50)

Список изменяющих документов
(в ред. Приказов ФСБ России от 29.01.2021 N 31,
от 02.02.2024 N 50)

ОБЩИЙ ВИД КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА
НА БУМАЖНОМ НОСИТЕЛЕ ДЛЯ ВЛАДЕЛЬЦА - ФИЗИЧЕСКОГО ЛИЦА

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

Сведения о владельце квалифицированного сертификата

Фамилия, имя, отчество (если имеется): <commonName>
Страховой номер индивидуального лицевого счета: <SNILS>
Идентификационный номер налогоплательщика: <INN>
Тип идентификации при выдаче сертификата: <identificationKind>

Сведения об издателе квалифицированного сертификата

Наименование удостоверяющего центра: <commonName>
Место нахождения удостоверяющего центра: <countryName>,
<stateOrProvinceName>, <localityName>, <streetAddress>
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>

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>
Действие ключа электронной подписи:
с <privateKeyUsagePeriod.notBefore>
по <privateKeyUsagePeriod.notAfter>

Электронная подпись под квалифицированным сертификатом

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

Подпись уполномоченного лица _____ / <расшифровка подписи>/

М.П.

<*> Символом "*" отмечено поле, которое в квалифицированном сертификате может отсутствовать.

Приложение N 2
к Требованиям (п. 32)

Список изменяющих документов
(в ред. Приказов ФСБ России от 29.01.2021 N 31,
от 02.02.2024 N 50)

**ОБЩИЙ ВИД КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА
НА БУМАЖНОМ НОСИТЕЛЕ ДЛЯ ВЛАДЕЛЬЦА - ЮРИДИЧЕСКОГО ЛИЦА**

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

Сведения о владельце квалифицированного сертификата

Наименование юридического лица: <commonName>
Основной государственный регистрационный номер: <OGRN>
Идентификационный номер налогоплательщика: <INNLE>
Место нахождения юридического лица: <countryName>,
<stateOrProvinceName>, <localityName>, <streetAddress>
* Физическое лицо, действующее от имени юридического лица без доверенности в соответствии с гражданским законодательством Российской Федерации: <title> <surname> <givenName>
* Идентификационный номер налогоплательщика физического лица, действующего от имени юридического лица без доверенности в соответствии с гражданским законодательством Российской Федерации: <INN>
* Страховой номер индивидуального лицевого счета физического лица, действующего от имени юридического лица без доверенности в соответствии с гражданским законодательством Российской Федерации: <SNILS>
Тип идентификации при выдаче сертификата: <identificationKind>

Сведения об издателе квалифицированного сертификата

Наименование удостоверяющего центра: <commonName>
Место нахождения удостоверяющего центра: <countryName>,
<stateOrProvinceName>, <localityName>, <streetAddress>
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>

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>
Действие ключа электронной подписи:
 с <privateKeyUsagePeriod.notBefore>
 по <privateKeyUsagePeriod.notAfter>

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 N 3
к Требованиям (п. 32)

Список изменяющих документов
(введено Приказом ФСБ России от 29.01.2021 N 31;
в ред. Приказа ФСБ России от 02.02.2024 N 50)

Общий вид квалифицированного сертификата
на бумажном носителе для владельца – физического лица,
являющегося индивидуальным предпринимателем

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

Сведения о владельце квалифицированного сертификата

Фамилия, имя, отчество (если имеется): <commonName>
Страховой номер индивидуального лицевого счета: <SNILS>
Идентификационный номер налогоплательщика: <INN>
Основной государственный регистрационный номер индивидуального
предпринимателя: <OGRNIP>
Тип идентификации при выдаче сертификата: <identificationKind>

Сведения об издателе квалифицированного сертификата

Наименование удостоверяющего центра: <commonName>
Место нахождения удостоверяющего центра: <countryName>,
<stateOrProvinceName>, <localityName>, <streetAddress>
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>

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>
Действие ключа электронной подписи:
с <privateKeyUsagePeriod.notBefore>
по <privateKeyUsagePeriod.notAfter>

Электронная подпись под квалифицированным сертификатом

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

Подпись уполномоченного лица _____/ <расшифровка подписи>/

М.П.

<*> Символом "*" отмечено поле, которое в квалифицированном сертификате может отсутствовать.

Приложение N 4
к Требованиям (п. 32)

Список изменяющих документов
(введено Приказом ФСБ России от 02.02.2024 N 50)

Общий вид квалифицированного сертификата
на бумажном носителе для владельца - лица, замещающего
государственные должности Российской Федерации, государственные
должности субъектов Российской Федерации, должностного лица
государственных органов, органов местного самоуправления,
их подведомственных учреждений, Центрального
банка Российской Федерации

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

Сведения о владельце квалифицированного сертификата

Фамилия, имя, отчество (если имеется): <commonName>
* Наименование органа (учреждения, Центрального банка Российской Федерации): <organizationName>
* Наименование подразделения органа (учреждения, Центрального банка Российской Федерации): <organizationUnitName>
Должность лица: <title>
Идентификационный номер налогоплательщика должностного лица: <INN>
Страховой номер индивидуального лицевого счета должностного лица: <SNILS>
Тип идентификации при выдаче сертификата: <identificationKind>

Сведения об издателе квалифицированного сертификата

Наименование удостоверяющего центра: <commonName>
Место нахождения удостоверяющего центра: <countryName>, <stateOrProvinceName>, <localityName>, <streetAddress>
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>

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>
Действие ключа электронной подписи: с <privateKeyUsagePeriod.notBefore>
по <privateKeyUsagePeriod.notAfter>

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 N 5
к Требованиям (п. 32)

(введено Приказом ФСБ России от 02.02.2024 N 50)

Общий вид квалифицированного сертификата
на бумажном носителе для владельца – филиала (представительства)
иностранного юридического лица

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

Сведения о владельце квалифицированного сертификата

Наименование филиала (представительства): <commonName>
Наименование иностранного юридического лица: <organizationName>
Идентификационный номер налогоплательщика иностранного юридического лица:
<INNLE>
Наименование филиала (представительства): <organizationUnitName>
Место нахождения филиала (представительства): <countryName>,
<stateOrProvinceName>, <localityName>, <streetAddress>
Руководитель филиала (представительства): <title>, <surname>, <givenName>
Идентификационный номер налогоплательщика руководителя: <INN>
Страховой номер индивидуального лицевого счета руководителя: <SNILS>
Тип идентификации при выдаче сертификата: <identificationKind>

Сведения об издателе квалифицированного сертификата

Наименование удостоверяющего центра: <commonName>
Место нахождения удостоверяющего центра: <countryName>,
<stateOrProvinceName>, <localityName>, <streetAddress>
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>

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>
Действие ключа электронной подписи: с <privateKeyUsagePeriod.notBefore>
по <privateKeyUsagePeriod.notAfter>

Электронная подпись под квалифицированным сертификатом

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

Подпись уполномоченного лица _____ /<расшифровка подписи>/

М.П.

<*> Символом "*" отмечено поле, которое в квалифицированном сертификате может отсутствовать.
