МИНИСТЕРСТВО ЭКОНОМИЧЕСКОГО РАЗВИТИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ (МИНЭКОНОМРАЗВИТИЯ РОССИИ)

П Р И К А З

_____ **Москва** № _____

Об установлении требований к сертификатам ключей проверки электронной подписи и ключам усиленной неквалифицированной электронной подписи, используемым в единой информационной системе в сфере закупок и на электронных площадках, в том числе с учетом обязательств, установленных международными договорами Российской Федерации

В соответствии с частью 3 статьи 5 Федерального закона от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (Собрание законодательства Российской Федерации, 2013, № 14, ст. 1652; № 27, ст. 3480; № 52, ст. 6961; 2014, № 23, ст. 2925; № 30, ст. 4225; № 48, ст. 6637; № 49, ст. 6925; 2015, № 1, ст. 51, ст. 72; № 10, ст. 1418) п р и к а з ы в а ю утвердить прилагаемые:

Требования к сертификатам ключей проверки электронной подписи и ключам усиленной неквалифицированной электронной подписи, используемым в единой информационной системе в сфере закупок и на электронных площадках.

Министр А.В. Улюкаев

УТВЕРЖДЕНЫ
приказом Минэкономразвития
России
от «____» _____ 2015 г.
№ ____

ТРЕБОВАНИЯ
к сертификатам ключей проверки электронной подписи и ключам усиленной электронной подписи, используемым в единой информационной системе и на электронных площадках

I. Общие положения

1. Настоящие Требования разработаны в соответствии с Федеральным законом от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

2. К настоящим Требованиям применимы термины и их определения, приведенные в указанных федеральных законах, а также:

ключевая информация – ключи электронной подписи и ключи проверки электронной подписи, действующие в течение определенного срока;

ключевой носитель – физический носитель определенной структуры, предназначенный для хранения ключевой информации ограниченного доступа (ключей электронной подписи), а при необходимости - контрольной, служебной и технологической информации;

ключевой документ – ключевой носитель, содержащий ключевую информацию ограниченного доступа.

II. Требования к сертификатам ключей проверки электронной подписи и ключам усиленной электронной подписи, используемым в единой информационной системе и на электронных площадках заказчиками, уполномоченными органами и уполномоченными учреждениями

3. Форма сертификатов ключей проверки электронной подписи, владельцами которых являются заказчики, уполномоченные органы и уполномоченные учреждения и используемых в единой информационной системе и на электронных площадках, должна удовлетворять требованиям приказа ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»
(далее – Приказ ФСБ России № 795), а также требованиям, установленным настоящим разделом Требований.

4. Сертификаты ключа проверки электронной подписи заказчиков, уполномоченных органов и уполномоченных учреждений должны включать дополнение «Улучшенный ключ» (2.5.29.37), в котором указываются сведения о полномочиях владельцев сертификатов ключей проверки электронных подписей:

1) полномочие в сфере размещения заказов, указываются следующие возможные значения:

заказчик;

уполномоченный орган;

уполномоченное учреждение.

2) полномочие пользователя единой информационной системы и электронных площадок, указываются следующие возможные значения:

администратор организации;

уполномоченный специалист;

специалист с правом согласования размещения заказа;

должностное лицо с правом подписи контракта (гражданско-правового

договора бюджетного учреждения, договора);

должностное лицо с правом подписи копии контракта (гражданско-правового договора бюджетного учреждения, договора);

специалист с правом направления проекта контракта (гражданско-правового договора бюджетного учреждения, договора) участнику закупки.

Сертификат ключа проверки может содержать несколько реквизитов, определяющих полномочия пользователя единой информационной системы.

Для полномочия в сфере размещения заказа "заказчик" возможно указание следующих полномочий пользователя официального сайта: "администратор организации", "уполномоченный специалист", "должностное лицо с правом подписи контракта (гражданско-правового договора бюджетного учреждения, договора)", "специалист с правом направления проекта контракта (гражданско-правового договора бюджетного учреждения, договора) участнику закупки".

Для полномочия в сфере размещения заказа «уполномоченный орган» или «уполномоченное учреждение» возможно указание следующих полномочий пользователя официального сайта: "администратор организации", "уполномоченный специалист", "специалист с правом согласования размещения заказа", "должностное лицо с правом подписи копии контракта (гражданско-правового договора бюджетного учреждения, договора)", "специалист с правом направления проекта контракта (гражданско-правового договора бюджетного учреждения, договора) участнику закупки".

5. Сертификаты ключей проверки электронной подписи и ключи электронной подписи, владельцами которых являются заказчики, уполномоченные органы и уполномоченные учреждения, должны использоваться совместно со средствами электронной подписи, сертифицированным ФСБ России (система сертификации – РОСС RU.0001.030001).

6. Ключи электронной подписи должны создаваться на ключевых носителях, предназначенных для хранения ключевой информации (смарт-

карты, usb-исполнение смарт-карты ("токен")). Данные ключевые носители должны поддерживаться применяемым средством электронной подписи.

7. Сроки действия сертификата ключа проверки электронной подписи и ключа электронной подписи не должны превышать максимальный срок действия, установленный для ключевых документов эксплуатационной документацией на используемое средство электронной подписи.

Сертификаты ключей проверки электронной подписи, владельцами которых являются заказчики, уполномоченные органы и уполномоченные учреждения, должны создаваться и выдаваться Удостоверяющим центром Федерального казначейства.

III.Требования к сертификатам ключей проверки электронной подписи и ключам усиленной электронной подписи, используемым в единой информационной системе и на электронных площадках участниками закупок, являющимися российскими юридическими и физическими лицами, в том числе, индивидуальными предпринимателями

8. Форма сертификатов ключей проверки электронной подписи, владельцами которых являются российские юридические и физические лица, в том числе. индивидуальные предприниматели (далее – российские участники закупок) и используемых в единой информационной системе и на электронных площадках, должна удовлетворять требованиям Приказа ФСБ России № 795, а также дополнительным требованиям, установленным настоящим разделом.

9. Сертификат ключа проверки электронной подписи российских участников закупок должен содержать следующие стандартные атрибуты имени:

1) «Неструктурированное имя» (UN, Unsructured Name) (1.2.840.113549.1.9.2), включающее:

INN=ИНН/KPP=КПП/OGRN=ОГРН - для юридических лиц (обязательное к заполнению);

INN=ИНН индивидуального предпринимателя – для индивидуального предпринимателя (обязательное к заполнению);

INN=ИНН физического лица - для физических лиц (обязательное к заполнению);

2) Компонент «Электронная почта» (E, EMail) (1.2.840.113549.1.9.1), содержащий адрес электронной почты владельца сертификата ключа проверки электронной подписи (обязательное к заполнению).

10. Сертификат ключа проверки электронной подписи российских физических лиц и российских индивидуальных предпринимателей должен содержать дополнительный атрибут имени INN (1.2.643.3.131.1.1) и включать ИНН данного физического лица.

11. Сертификат ключа проверки электронной подписи российских индивидуальных предпринимателей должен содержать дополнительный атрибут имени OGRNIP (1.2.643.100.5) и включать общероссийский государственный регистрационный номер индивидуального предпринимателя.

12. Сертификат ключа проверки электронной подписи российских участников закупок должен включать дополнение «Улучшенный ключ» (2.5.29.37). В данное дополнении должны быть указаны идентификатор объекта 1.3.6.1.5.5.7.3.2 – «Проверка подлинности клиента» и идентификатор объекта 1.3.6.1.5.5.7.3.4 – «Защищенная электронная почта», а также сведения о полномочиях использования сертификата ключа проверки электронной подписи на электронных площадках:

1) Идентификатор объекта 1.2.643.6.3.1.1 - Использование на электронных площадках, отобранных для проведения аукционов в электронной форме;

2) Тип участника (один вариант из списка):

Юридическое лицо (OID 1.2.643.6.3.1.2.1);

Физическое лицо (OID 1.2.643.6.3.1.2.2);

Индивидуальный предприниматель (OID 1.2.643.6.3.1.2.3);

3) Тип организации: Участник закупки (OID 1.2.643.6.3.1.3.1);

4) Полномочия (множественный выбор):

Администратор организации (OID 1.2.643.6.3.1.4.1);

Уполномоченный специалист (OID 1.2.643.6.3.1.4.2);

Специалист с правом подписи контракта(OID 1.2.643.6.3.1.4.3)

13. Сертификат ключа проверки электронной подписи российских участников закупки должен включать дополнение «Точка распространения списка отозванных сертификатов» (2.5.29.31), содержать протоколы доступа и адреса публикации списка отозванных сертификатов, на основании которого может быть установлен статус данного сертификата ключа проверки электронной подписи.

14. Стандартные и дополнительные атрибуты имени сертификата ключа проверки электронной подписи российских участников закупки должны заполняться на русском языке с использованием символов кириллического алфавита.

15. Сертификаты ключей проверки электронной подписи и ключи электронной подписи, владельцами которых являются российские участники закупок, должны использоваться совместно со средствами электронной подписи, - сертифицированными ФСБ России (система сертификации – РОСС RU.0001.030001).16.Ключи электронной подписи должны создаваться на ключевых носителях, предназначенных для хранения ключевой информации (смарт-карты, usb-исполнение смарт-карты ("токен")). Данные ключевые носители должны поддерживаться применяемым средством электронной подписи.

17. Сроки действия сертификата ключа проверки электронной подписи и ключа электронной подписи не должны превышать максимальный срок действия, установленный для ключевых документов эксплуатационной документацией на используемое средство электронной подписи.

18. Сертификаты ключей проверки электронной подписи, владельцами которых являются российские участники закупок, должны создаваться и выдаваться авторизованными для работы в единой информационной системе и торговыми площадками удостоверяющими центрами.

IV. Требования к сертификатам ключей проверки электронной подписи и ключам усиленной электронной подписи, используемым в единой информационной системе и на электронных площадках участниками закупки, являющимися иностранными юридическими и физическими лицами, в том числе иностранными индивидуальными предпринимателями

19. Форма сертификатов ключей проверки электронной подписи, владельцами которых являются иностранные юридические и физические лица, в том числе иностранные индивидуальные предприниматели (далее – иностранный участник закупок) и используемых в единой информационной системе и на электронных площадках, должна соответствовать стандарту X.509v3 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile" и иметь следующую структуру:

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	Наименование алгоритма электронной подписи
Issuer	Издатель сертификата	Аттрибуты имени Удостоверяющего центра – издателя сертификата
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	Атрибуты имени владельца сертификата
Public Key	Открытый ключ	Ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	Наименование алгоритма электронной подписи Удостоверяющего центра - издателя сертификата
Issuer Sign	ЭЦП издателя сертификата	Электронная подпись Удостоверяющего центра - издателя сертификата
Расширения сертификата		
Key Usage	Использование ключа	Информация об использовании ключа. Значение данного поля должно обеспечивать использование ключа для формирования электронной подписи и шифрования данных
Extended Key Usage	Улучшеный ключ	Указываются идентификаторы областей использования ключей подписи

Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор ключа подписи - владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор ключа подписи Удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/Name.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, Name - имя файла списка отозванных сертификатов.
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 5280

20. Сертификат ключа проверки электронной подписи иностранного участника закупок должен содержать следующие атрибуты имени владельца (поле Subject):

1) компонент «Общее имя» (CommonName, 2.5.4.3), содержащий:

наименование юридического лица – для юридического лица (обязательное

к заполнению);

фамилию, имя, отчество (если имеется) – для физического лица и индивидуального предпринимателя (обязательное к заполнению);

2) компонент «Фамилия» (SurName, 2.5.4.4), содержащий:

фамилия полномочного представителя юридического лица по работе в единой информационной системе и на торговых площадках - для юридического лица (обязательное к заполнению);

фамилия – для физического лица и индивидуального предпринимателя (необязательное к заполнению);

3) компонент «Приобретенное имя» (GivenName, 2.5.4.42), содержащий:

имя и отчество (если есть) полномочного представителя юридического лица по работе в единой информационной системе и на торговых площадках - для юридического лица (обязательное к заполнению);

имя и отчество (если имеется) – для физического лица и индивидуального предпринимателя (необязательное к заполнению);

4) компонент «Наименование организации» (OrganizationName, 2.5.4.10), содержащий:

наименование юридического лица – для юридического лица (обязательное

к заполнению);

наименование индивидуального предпринимателя - для индивидуальных предпринимателей (обязательное к заполнению);

не заполняется - для физических лиц;

5) компонент «Должность» (Title, 2.5.4.12), содержащий:

должность полномочного представителя юридического лица по работе в единой информационной системе и на торговых площадках - для юридического лица (обязательное к заполнению);

не заполняется – для индивидуальных предпринимателей и физических лиц;

6) компонент «Наименование населенного пункта» (LocalityName, 2.5.4.12), содержащий наименование населённого пункта, где зарегистрировано юридическое лицо, индивидуальный предприниматель, физическое лицо (обязательное к заполнению);

7) компонент «Наименование штата или области» (StateOrProvinceName, 2.5.4.8), содержащий название региона, где зарегистрировано юридическое лицо, индивидуальный предприниматель, физическое лицо (обязательное к заполнению);

8) компонент «Наименование страны» (CountryName, 2.5.4.6), содержащее двухзначный код страны (например, «BY»), в которой зарегистрировано юридическое лицо, индивидуальный предприниматель, физическое лицо (обязательное к заполнению);

9) компонент «Электронная почта» (EMail, 1.2.840.113549.1.9.1), содержащий адрес электронной почты владельца сертификата ключа подписи (обязательное к заполнению).

21. Сертификат ключа проверки электронной подписи иностранного

участника закупок должен включать дополнение «Улучшенный ключ» (2.5.29.37) и содержать:

1) Идентификатор объекта 1.3.6.1.5.5.7.3.2 – «Проверка подлинности клиента»;

2) Идентификатор объекта 1.3.6.1.5.5.7.3.4 - «Защищенная электронная почта»,

22. В сертификат ключа проверки электронной подписи иностранного участника закупок также могут включаться сведения о полномочиях использования сертификата ключа проверки электронной подписи на электронных площадках:

1) Идентификатор объекта 1.2.643.6.3.1.1 - Использование на электронных площадках, отобранных для проведения аукционов в электронной форме;

2) Тип участника (один вариант из списка):

Юридическое лицо (OID 1.2.643.6.3.1.2.1);

Физическое лицо (OID 1.2.643.6.3.1.2.2);

Индивидуальный предприниматель (OID 1.2.643.6.3.1.2.3);

3) Тип организации: Участник закупки (OID 1.2.643.6.3.1.3.1);

4) Полномочия (множественный выбор):

Администратор организации (OID 1.2.643.6.3.1.4.1);

Уполномоченный специалист (OID 1.2.643.6.3.1.4.2);

Специалист с правом подписи контракта(OID 1.2.643.6.3.1.4.3).

23. В случае, если в сертификате ключа проверки электронной подписи иностранного участника закупок в дополнении «Улучшенный ключ» (2.5.29.37) отсутствуют идентификаторы объекта, устанавливающие тип участника, то тип данного участника устанавливается на основе значения атрибута имени «Общее имя» (CommonName, 2.5.4.3) по следующему правилу:

1) если в этом атрибуте указано наименование организации, то тип участника – юридическое лицо;

2) если указано фамилия, имя и отчество, а атрибут имени «Наименование организации» (OrganizationName, 2.5.4.10) не заполнен, то тип участника – физическое лицо;

3) если указано фамилия, имя и отчество, а атрибут имени «Наименование организации» (OrganizationName, 2.5.4.10) заполнен (содержит наименование индивидуального предпринимателя), то тип участника – индивидуальный предприниматель.

24. В случае, если в сертификате ключа проверки электронной подписи иностранного участника закупок в дополнении «Улучшенный ключ» (2.5.29.37) отсутствуют идентификаторы объекта, устанавливающие полномочия, признается, что владелец данного сертификата наделен всеми приведенными полномочиями.

25. Сертификат ключа проверки электронной подписи иностранных участников закупки должен включать дополнение «Точка распространения списка отозванных сертификатов» (2.5.29.31), содержать протоколы доступа и адреса публикации списка отозванных сертификатов, на основании которого может быть установлен статус данного сертификата ключа проверки электронной подписи.

26. Атрибуты компонент имени, а также иные поля и расширения сертификата ключа проверки электронной подписи иностранных участников закупок рекомендуется заполнять на русском языке. В случае, если сертификат ключа проверки электронной подписи включает атрибуты компонент имени, а также иные поля и расширения, заполненные на языке, отличном от русского, то участник закупок при регистрации в единой информационной системе или при аккредитации на торговой площадке, а также в случае смены сертификата ключа проверки электронной подписи обязан предоставить перевод на русский язык сертификата ключа проверки электронной подписи, заверенный установленным порядком.

27. Если сертификаты ключей проверки электронной подписи и ключи

электронной подписи, владельцами которых являются иностранные участники закупок, изготовлены и выданы российскими удостоверяющими центрами, то они должны использоваться совместно со средствами электронной подписи, получившими подтверждение соответствия требованиям, установленным Федеральным законом Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" (средствами электронной подписи, сертифицированными ФСБ России на соответствие положений Приказа ФСБ России от 27.12.2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра).

28. При создании и выдаче сертификата ключа проверки электронной подписи иностранным удостоверяющем центром сертификаты ключей проверки электронной подписи и ключи электронной подписи, владельцами которых являются иностранные участники закупок, должны использоваться совместно со средствами электронной подписи, удовлетворяющим положениям статьи 12 Федерального закона Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

29. Ключи электронной подписи должны создаваться на ключевых носителях, предназначенных для хранения ключевой информации (смарт-карты, usb-исполнение смарт-карты ("токен")). Данные ключевые носители должны поддерживаться применяемым средством электронной подписи.

30. Сроки действия сертификата ключа проверки электронной подписи и ключа электронной подписи не должны превышать максимальный срок действия, установленный для ключевых документов эксплуатационной документацией на используемое средство электронной подписи.

31. Сертификаты ключей проверки электронной подписи, владельцами которых являются иностранные участники закупок, должны создаваться и выдаваться авторизованными для работы в единой информационной системе и торговыми площадками российскими и иностранными удостоверяющими центрами.

V.Требования к форме списка отозванных сертификатов, формируемого удостоверяющими центрами в целях обеспечения установления статуса сертификатов ключей проверки электронной подписи, использующихся в единой информационной системе и на электронных площадках

32. Форма списка отозванных сертификатов, издаваемого удостоверяющим центром, должна соответствовать стандарту X.509v2 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile"и иметь следующую структуру:

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	Аттрибуты имени Удостоверяющего центра – издателя списка отозванных сертификатов
thisUpdate	Время изготовления СОС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы
signatureAlgorithm	Алгоритм подписи	Наименование алгоритма электронной подписи
Issuer Sign	Подпись издателя СОС	Значение электронной подписи, сформированной по алгоритму signatureAlgorithm
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа подписи Удостоверяющего центра, на котором подписан список отозванных сертификатов
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата ключа проверки электронной подписи Удостоверяющего центра (не обязательный атрибут)
CRLNumber	Номер СОС	Порядковый номер выпущенного СОС

		(не обязательный атрибут)
		В список отозванных сертификатов могут быть добавлены дополнительные поля и расширения согласно RFC 5280