МИНИСТЕРСТВО ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ КАЗНАЧЕЙСТВО
(КАЗНАЧЕЙСТВО РОССИИ)

ПРИКАЗ

23 декабря 2011 г. № 621

Москва

Об утверждении регламента организации работы с сертификатами ключей проверки электронных подписей

В соответствии с приказом Министерства финансов Российской Федерации от 21 июля 2011 г. № 86н «Об утверждении порядка предоставления информации государственным (муниципальным) учреждением, ее размещения на официальном сайте в сети Интернет и ведения указанного сайта» и совместным приказом Министерства экономического развития Российской Федерации и Федерального казначейства от 14.12.2010 № 647/22н «Об утверждении Порядка регистрации пользователей на официальном сайте Российской Федерации в сети Интернет для размещения информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг», п р и к а з ы в а ю:

1. Утвердить прилагаемый Регламент организации работы с сертификатами ключей проверки электронных подписей.

2. Настоящий приказ вступает в силу с 1 января 2012 года.

Руководитель Р.Е. Артюхин

УТВЕРЖДЕН
приказом Федерального казначейства
от 23.12.2011 № 621

Регламент
организации работы с сертификатами
ключей проверки электронных подписей

1. Термины и определения

1.1. Автоматизированное рабочее место (далее – АРМ) – программно-технические средства, предназначенные для работы с официальным сайтом.

1.2. 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.

1.3. Владелец сертификата – лицо, которому в установленном настоящим регламентом порядке выдан сертификат ключа проверки ЭП.

1.4. Запрос – электронный документ, содержащий ключ проверки ЭП, сведения о владельце сертификата и иные реквизиты.

1.5. Ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП.

1.6. Ключ ЭП – уникальная последовательность символов, предназначенная для создания электронной подписи.

1.7. Компрометация ключа ЭП – событие, определенное владельцем сертификата, как ознакомление неуполномоченным лицом (лицами) с его ключом электронной подписи, хищение, утеря носителя ключевой информации, несанкционированное копирование или другие причины появления у владельца сертификата сомнений в сохранении тайны ключа ЭП.

1.8. Уполномоченный удостоверяющий центр Федерального казначейства (далее – УУЦ) – основной компонент инфраструктуры ключей проверки подписей Федерального казначейства, осуществляющий выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ.

1.9. Корневой сертификат УУЦ – сертификат центра сертификации УУЦ, используемый для проверки достоверности сертификатов, выданных УУЦ, других пользователей.

1.10. Носитель ключевой информации – носитель информации, используемый для хранения ключа ЭП.

1.11. Региональный центр регистрации (далее – РЦР) – подчиненный УУЦ компонент инфраструктуры ключей проверки подписей Федерального казначейства, осуществляющий обработку регистрационной информации

владельцев сертификатов и авторизацию запросов в органе Федерального казначейства.

1.12. Оператор РЦР – Уполномоченное лицо УУЦ, занимающееся рассмотрением и обработкой заявлений на изготовление, аннулирование, приостановление/возобновление действия сертификатов выданных УУЦ.

1.13. Организатор – территориальный орган Федерального казначейства.

1.14. Аннулирование сертификата – процедура отзыва сертификата, до истечения срока его действия. Восстановление действия аннулированного сертификата невозможно.

1.15. Официальный сайт – Официальный сайт Российской Федерации в сети «Интернет» для размещения информации о государственных (муниципальных) учреждениях или Официальный сайт Российской Федерации в информационно-телекоммуникационной сети "Интернет" для размещения информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг.

1.16. Электронный документ (далее – ЭД) – документ, в котором информация представлена в электронной форме.

1.17. Полномочное должностное лицо Участника – сотрудник Участника, которому руководителем Участника делегировано право определять полномочия сотрудников по подписанию ЭД ЭП при работе на Официальном сайте.

1.18. Сертификат – сертификат ключа проверки ЭП, выданный УУЦ.

1.19. Средства криптографической защиты информации (далее – СКЗИ) – программные средства криптографической защиты информации, обеспечивающие применение ЭП при осуществлении электронного документооборота.

1.20. Уполномоченное лицо УУЦ – сотрудник Федерального казначейства, наделенный правом заверения сертификатов, изданных центром сертификации УУЦ.

1.21. Уполномоченное лицо Участника – сотрудник Участника, наделенный полномочиями по подписанию документов ЭП.

1.22. Участник – учреждение (организация), представившая в установленном порядке в орган Федерального казначейства необходимые документы для работы на Официальном сайте.

2. Общие положения

2.1. Настоящий Регламент определяет основные правила получения и использования сертификатов уполномоченными лицами Участника.

2.2. Мероприятия по управлению сертификатами (выдача, аннулирование, приостановление/возобновление действия) осуществляются РЦР, в случае положительного результата проверки документов, представленных в установленном порядке Участником Организатору для работы на Официальном сайте.

3. Подготовительные мероприятия

3.1. Организатор передает Участнику во временное пользование:

– ПО для формирования ключей ЭП, файлов запросов и заявлений на получение сертификатов (Приложение № 1 к настоящему Регламенту) [1];

– СКЗИ (в порядке, установленном Организатором);

– Эксплуатационную документацию на передаваемое ПО и СКЗИ.

3.2. Участник обеспечивает установку переданного в соответствии с п. 3.2.2 настоящего Регламента ПО.

3.3. Участник, используя полученное от Организатора ПО, обеспечивает формирование ключей ЭП, файла запроса, распечатку и подпись заявлений на получение сертификатов уполномоченными лицами Участника, заверяет их собственноручной подписью руководителя (или полномочного должностного лица) Участника и печатью Участника.

4. Порядок первичного получения сертификатов

4.1. Для первичного получения сертификата уполномоченное лицо Участника представляет в РЦР:

4.1.1. Файл Запроса на сертификат[2] на съемном носителе информации (дискета или др.) на издание сертификата;

4.1.2. Заявление на получение сертификата на бумажном носителе (Приложение № 1 к настоящему Регламенту);

4.1.3. Документ, удостоверяющий личность уполномоченного лица Участника (его доверенного лица);

4.1.4. Заверенную копию приказа о назначении полномочного должностного лица Участника (в случае, если заявление на получение сертификата заверено не руководителем Участника);

4.1.5. Оформленную в установленном порядке от уполномоченного лица Участника доверенность (при получении сертификата по доверенности).

4.2. В случае не предъявления указанных в п. 4.1 документов или несоответствии данных Запроса сведениям, представленным в заявлении на получение сертификата, уполномоченному лицу Участника отказывается в выдаче сертификата.

4.3. В течение 5-х рабочих дней после представления документов уполномоченное лицо Участника информируется о готовности сертификата по электронной почте, адрес которой указан в Запросе, либо другим согласованным с уполномоченным лицом Участника способом.

4.4. После издания сертификата уполномоченному лицу Участника передаются:

---

[1] Съёмный носитель для записи ПО предоставляется Участником

[2] Формируется на этапе генерации ключей ЭП, используя ПО, переданное Участнику

– электронные копии файла сертификата и файла корневого сертификата УУЦ (на съемном носителе информации, предоставляемом уполномоченным лицом Участника);

– две бумажных копии сертификата, заверенные подписью Оператора РЦР и печатью УУЦ, для подписи уполномоченным лицом Участника (один экземпляр сертификата с подписью уполномоченного лица Участника возвращается Оператору РЦР, в случае непредставления бумажной копии сертификата в течение 10 дней – сертификат уполномоченного лица Участника приостанавливается РЦР, до момента получения подписанного экземпляра сертификата).

4.5. Участник обеспечивает установку полученных в РЦР файлов сертификатов на АРМ, с которого будет осуществляться работа с Официальным сайтом, и выполнение настроек согласно эксплуатационной документации.

5. Порядок плановой смены сертификатов

5.1. Плановая смена сертификатов осуществляется в течение 10 рабочих дней до окончания срока их действия по обращению Владельца сертификата (или его доверенного лица) в РЦР по месту получения сертификата.

5.2. Для плановой смены сертификата Владельцу сертификата (или его доверенному лицу) необходимо представить в РЦР сформированный с использованием ПО, указанного в пункте 3.1 настоящего Регламента, Запрос на съемном носителе информации и Заявление на получение сертификата. При наличии подключения Участника к системе электронного документооборота (далее – СЭД) Федерального казначейства допускается направлять Запрос в РЦР, подписанный ЭП Владельца сертификата и руководителя (или полномочного должностного лица) Участника в электронном виде.

5.3. В течение 5-х рабочих дней после представления документов уполномоченное лицо Участника информируется о готовности сертификата по электронной почте, адрес которой указан в Запросе, либо другим согласованным с уполномоченным лицом Участника способом.

5.4. Получение и установка сертификата в рамках плановой смены осуществляется в порядке согласно п.п. 4.4 и 4.5 настоящего Регламента.

6. Порядок аннулирования сертификата

6.1. Осуществляется аннулирование сертификата в случаях:

–компрометации ключа ЭП;

–изменения сведений или полномочий Владельца сертификата или Участника, указанных в сертификате;

–прекращения полномочий Владельца сертификата;

– выхода из строя носителя ключевой информации.

6.2. Аннулирование сертификата при компрометации ключа ЭП.

Запрещается использовать скомпрометированные ключи ЭП для подписи ЭД. ЭД, подписанный скомпрометированным ключом ЭП, считается недействительным и не исполняется.

6.3. При компрометации или подозрении на компрометацию своего ключа ЭП Владелец сертификата должен незамедлительно по телефону заявить в РЦР, выдавший сертификат, об аннулировании сертификата, сообщив причину аннулирования, серийный номер сертификата и номер идентификатора ключей при смене, указанный в бумажной копии соответствующего сертификата.

6.4. При сообщении корректного номера идентификатора ключей Владельца сертификата, действие сертификата приостанавливается. В противном случае РЦР имеет право отказать в приостановлении действия сертификата до получения соответствующего письменного заявления.

6.5. В день обращения в РЦР Владелец сертификата скомпрометированного ключа ЭП должен направить в РЦР, выдавший сертификат, письменное заявление на аннулирование сертификата по форме согласно Приложению № 2 к настоящему Регламенту с указанием даты аннулирования, причины аннулирования и серийного номера сертификата, заверенное подписью руководителя (или полномочного должностного лица) Участника и печатью Участника. В случае, если заявление на аннулирование сертификата не будет представлено, РЦР вправе отказать Владельцу сертификата в получении нового сертификата.

6.6. Получение нового сертификата осуществляется аналогично п.п. 5.2 – 5.4 настоящего Регламента.

6.7. При изменении сведений или полномочий владельца, указанных в сертификате, аннулирование сертификата осуществляется по письменному заявлению владельца на аннулирование сертификата, представленному в РЦР, где был выдан сертификат, заверенному подписью руководителя (или полномочного должностного лица) Участника и печатью Участника.

6.8. При прекращении полномочий Владельца сертификата аннулирование сертификата осуществляется по письменному заявлению, представленному в РЦР, где был выдан сертификат, заверенному подписью руководителя (или полномочного должностного лица) Участника и печатью Участника. При наличии подключения Участника к СЭД Федерального казначейства допускается направлять заявление об аннулировании сертификата в электронном виде с подписью руководителя (или полномочного должностного лица) Участника.

6.9. При выходе из строя носителя ключевой информации аннулирование сертификата осуществляется по письменному заявлению Владельца сертификата, представленному в РЦР, где был выдан сертификат, заверенному подписью руководителя (или полномочного должностного лица) Участника и печатью Участника.

7. Порядок приостановления действия сертификата

7.1. Приостановление действия сертификата может осуществляться по инициативе Владельца сертификата на период возможного длительного неисполнения обязанностей, связанных с подписанием ЭД, или по инициативе Организатора в случае непредставления Участником информации об изменении реквизитов Участника.

7.2. Приостановление действия сертификата на период возможного длительного неисполнения обязанностей, связанных с подписанием ЭД, осуществляется по письменному заявлению Владельца сертификата, представленному в РЦР по форме согласно Приложению № 2 к настоящему Регламенту, где был выдан сертификат, с указанием даты, причины приостановления действия сертификата и его серийного номера, заверенному подписью руководителя (или полномочного должностного лица) Участника и печатью Участника. При наличии подключения Участника к СЭД Федерального казначейства допускается направлять заявление о приостановлении действия сертификата в электронном виде с электронными подписями Владельца сертификата и руководителя (или полномочного должностного лица) Участника.

8. Порядок возобновления действия сертификатов

8.1. Возобновление действия сертификата после приостановления его действия по инициативе Организатора в случае непредставления информации об изменении реквизитов Участника или в случае непредставления бумажной копии сертификата осуществляется после получения Организатором соответствующих документов, оформленных в установленном порядке.

8.2. Возобновление действия сертификата после приостановления его действия по инициативе Участника на период длительного неисполнения Владельцем сертификата обязанностей, связанных с подписанием ЭД, осуществляется по письменному заявлению Владельца сертификата, в РЦР, где был выдан сертификат, заверенному подписью руководителя (или полномочного должностного лица) Участника и печатью Участника.

Приложение № 1
к Регламенту
организации работы
с сертификатами
ключей проверки
электронных
подписей

Заявление на получение в Уполномоченном удостоверяющем центре Федерального казначейства сертификата ключа проверки электронной подписи

В связи с _____,
предоставлением права использования ЭП, плановой сменой, изменением реквизитов владельца или указать другую причину

прошу выдать сертификат ключа проверки электронной подписи (ЭП) для работы со средством криптографической защиты информации (СКЗИ) **КриптоПро CSP** участнику информационной системы:

Фамилия, имя, отчество

Организация

Полномочие Участника в сфере размещения заказов

Полномочия Участника на Официальном сайте ГМУ

Должность

Подразделение

Полномочия владельца [3]

ИНН

КПП

ОГРН

Код организации в сводном перечне заказчиков

Код организации в реестре организаций сектора государственного управления

На основании _____
(указать исх.№ служебной записки, приказа о предоставлении полномочий начальника Управления, Руководителя)

_____ от "___" _____ 20 ____ г. № _____

работнику предоставлены полномочия на эксплуатацию СКЗИ и использование ЭП при электронном документообороте.

Алгоритм открытого ключа:
Распечатка значения ключа проверки ЭП пользователя:

Алгоритм подписи запроса:

---

[3] В данном поле указывается полный список полномочий пользователя (владельца сертификата ключа ЭП) в системах Федерального казначейства, в которых может использоваться данный сертификат

Распечатка значения подписи запроса:

Сведения об отношениях, при осуществлении которых электронный документ с ЭП будет иметь юридическое значение:

- недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе

Расширенное назначение сертификата ключа проверки ЭП:

- ЭП документа

Наименование средств ЭП, с которыми используется данный ключ проверки ЭП:

- СКЗИ КриптоПро CSP

Назначение сертификата[4]:

- Сертификат предназначен для обмена электронными документами с Общероссийским официальным сайтом(OID).
- Сертификат предназначен для обмена электронными документами с Официальным сайтом ГМУ(OID).
- Сертификат предназначен для АРМ СЭД (OID).
- Сертификат предназначен для внутриведомственного документооборота (OID).

Владелец ключей ЭП _____

Подпись

"___" _____ 20____ г.

Директор (Руководитель) _____

_____ / _____

М.П. Подпись

"___" _____ 20____ г.

[4] *Курсивом* приведены примеры значений Назначения сертификата. Полный перечень возможных значений приведён в документе «Правила пользования единым универсальным сертификатом»

Приложение № 2
к Регламенту
организации
работы с
сертификатами
ключей проверки
электронных
подписей

Заявление на аннулирование (приостановление действия)
в Уполномоченном удостоверяющем центре
Федерального казначейства
сертификата ключа проверки электронной подписи

В связи с _____
увольнением, изменением реквизитов владельца, уходом в отпуск или указать другую причину
прошу отозвать (приостановить действие) сертификат(а) ключа проверки электронной подписи (сертификат).
Наименование организации (сокращенное/краткое):_____
Фамилия, Имя, Отчество:_____
Должность:_____
Отдел:_____
Управление:_____
Контактный телефон:_____
Дата выдачи сертификата:_____
Дата приостановления действия сертификата:_____
Серийный номер:_____
Владелец сертификата: _____ "___" _____ 20____ г.
Подпись
Руководитель организации:_____ "___" _____ 20____ г.
Подпись Расшифровка

МП "___" _____ 20____ г.