ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 1 декабря 2021 г. № 2152

МОСКВА

Об утверждении Правил создания и использования сертификата ключа проверки усиленной неквалифицированной электронной подписи в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме

Правительство Российской Федерации **п о с т а н о в л я е т :**

Утвердить прилагаемые Правила создания и использования сертификата ключа проверки усиленной неквалифицированной электронной подписи в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.

Председатель Правительства
Российской Федерации М.Мишустин

5346386

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от 1 декабря 2021 г. № 2152

П Р А В И Л А

создания и использования сертификата ключа проверки усиленной неквалифицированной электронной подписи в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме

1. Настоящие Правила устанавливают порядок создания и использования сертификата ключа проверки усиленной неквалифицированной электронной подписи (далее - сертификат ключа проверки электронной подписи) в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме (далее - инфраструктура электронного правительства).

Сертификаты ключей проверки электронной подписи создаются аккредитованным удостоверяющим центром, владеющим специализированной защищенной автоматизированной системой, соответствующей требованиям, указанным в пунктах 14 и 15 настоящих Правил (далее соответственно - удостоверяющий центр, автоматизированная система), с использованием средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным Федеральной службой безопасности Российской Федерации на основании модели угроз безопасности информации, указанной в пункте 13 настоящих Правил.

2. Инфраструктура электронного правительства обеспечивает жизненный цикл сертификатов ключей проверки электронной подписи, владельцами (пользователями) которых выступают физические лица, а также физические лица при представлении интересов индивидуальных предпринимателей и юридических лиц (при наличии доверенностей,

подтверждающих их полномочия) при наличии у них учетной записи в 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" (далее - единая система идентификации и аутентификации) и ключа простой электронной подписи, выданного при личном приеме в соответствии с Правилами использования простой электронной подписи при оказании государственных и муниципальных услуг, утвержденными постановлением Правительства Российской Федерации от 25 января 2013 г. № 33 "Об использовании простой электронной подписи при оказании государственных и муниципальных услуг" (далее - подтвержденная учетная запись в единой системе идентификации и аутентификации).

3. Реализация функций по созданию сертификатов ключей проверки электронной подписи осуществляется удостоверяющим центром.

4. Для обеспечения функций по созданию и применению сертификатов ключей проверки электронной подписи и соответствующих им ключей усиленной неквалифицированной электронной подписи при обеспечении электронного взаимодействия пользователей с автоматизированной системой по защищенным протоколам связи с использованием российских криптографических алгоритмов применяются сертификаты специального вида, позволяющие аутентифицировать взаимодействующих субъектов и устанавливать криптографически защищенное соединение (далее - сертификат безопасности).

5. Для подписания сертификатов ключей проверки электронной подписи пользователей используется ключ усиленной неквалифицированной электронной подписи удостоверяющего центра, ключ проверки которой содержится в сертификате ключа проверки электронной подписи удостоверяющего центра, подписанном усиленной неквалифицированной электронной подписью удостоверяющего центра, основанной на сертификате ключа проверки электронной подписи, или сертификате ключа проверки электронной подписи, выданном удостоверяющему центру информационной системой головного удостоверяющего центра, функции которого осуществляет уполномоченный федеральный орган исполнительной власти в соответствии с абзацем четвертым подпункта "а" пункта 2 Положения

об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, утвержденного постановлением Правительства Российской Федерации от 8 июня 2011 г. № 451 "Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме".

6. Для подписания сертификатов безопасности используется ключ усиленной неквалифицированной электронной подписи, ключ проверки которой содержится в сертификате ключа проверки электронной подписи, подписанном усиленной неквалифицированной электронной подписью удостоверяющего центра, основанной на сертификате ключа проверки электронной подписи, и отличном от указанного в пункте 5 настоящих Правил.

7. Реализация электронного взаимодействия с автоматизированной системой и с единой системой идентификации и аутентификации обеспечивается по защищенным протоколам связи с поддержкой российских криптографических алгоритмов.

8. Создание ключей усиленной неквалифицированной электронной подписи и ключей проверки усиленной неквалифицированной электронной подписи, запросов на создание и выдачу сертификатов ключей проверки электронной подписи, подписание электронных документов усиленной неквалифицированной электронной подписью и проверка усиленной неквалифицированной электронной подписи в электронном документе производится пользователем с использованием средств электронной подписи и средств криптографической защиты информации, имеющих подтверждение соответствия требованиям, установленным Федеральной службой безопасности Российской Федерации на основании модели угроз безопасности информации, указанной в пункте 13 настоящих Правил (далее - защищенные средства электронной подписи и защиты информации). Защищенные средства электронной подписи и защиты информации функционируют в составе клиентской части автоматизированной системы - мобильном приложении или могут быть установлены на стационарных средствах вычислительной техники (при наличии технической возможности).

9. Защищенные средства электронной подписи и защиты информации, функционирующие в составе мобильного приложения или устанавливаемые на стационарных средствах вычислительной техники, предоставляются пользователям на безвозмездной основе через информационные ресурсы инфраструктуры электронного правительства или информационные ресурсы производителей мобильных операционных систем.

10. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации обеспечивает ведение реестра выданных сертификатов ключей проверки электронной подписи посредством размещения в федеральной государственной информационной системе "Единый портал государственных и муниципальных услуг (функций)" (далее - единый портал).

11. Удостоверяющий центр обеспечивает ведение публичных информационных ресурсов в целях распространения сведений о досрочно прекративших действие и аннулированных сертификатах ключей проверки электронной подписи, выданных удостоверяющим центром.

12. Проверка усиленной неквалифицированной электронной подписи, созданной в соответствии с настоящими Правилами, производится пользователями самостоятельно либо с использованием сервиса проверки усиленной неквалифицированной электронной подписи в инфраструктуре электронного правительства, реализованного указанным в пункте 5 настоящих Правил головным удостоверяющим центром или доверенной третьей стороной.

13. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации определяет по согласованию с Федеральной службой безопасности Российской Федерации модель угроз безопасности информации, обрабатываемой в автоматизированной системе.

14. Федеральная служба безопасности Российской Федерации на основании модели угроз безопасности информации, обрабатываемой в автоматизированной системе, определяет требования к автоматизированной системе.

15. До определения требований, указанных в пункте 14 настоящих Правил, к автоматизированной системе предъявляются требования, разработанные и утвержденные в рамках реализации постановления Правительства Российской Федерации от 29 октября 2016 г. № 1104 "О проведении в 2016 - 2018 годах эксперимента в целях обеспечения направления электронных документов для государственной регистрации

юридических лиц и индивидуальных предпринимателей и открытия им счетов в кредитных организациях с использованием специализированной защищенной автоматизированной системы, предназначенной для централизованного создания и хранения ключей усиленной квалифицированной электронной подписи, а также их дистанционного применения владельцами квалифицированных сертификатов ключа проверки электронной подписи".

16. Выдача пользователю сертификата ключа проверки электронной подписи осуществляется при наличии в единой системе идентификации и аутентификации фамилии, имени, отчества (при наличии), страхового номера индивидуального лицевого счета, идентификационного номера налогоплательщика, серии и номера основного документа, удостоверяющего личность, даты рождения, абонентского номера подвижной радиотелефонной связи либо при представлении этих сведений пользователем (в случае их отсутствия в подтвержденной учетной записи в единой системе идентификации и аутентификации). В случае отсутствия в подтвержденной учетной записи в единой системе идентификации и аутентификации указанных сведений сертификат ключа проверки электронной подписи удостоверяющим центром не выдается.

17. Для формирования запросов на создание и выдачу сертификата ключа проверки электронной подписи и сертификата безопасности пользователем используются защищенные средства электронной подписи и защиты информации.

18. После загрузки защищенных средств электронной подписи и защиты информации на устройство подвижной радиотелефонной связи пользователь проходит процедуру регистрации и процедуру аутентификации пользователя через единую систему идентификации и аутентификации. Далее автоматизированная система получает из единой системы идентификации и аутентификации персональные данные пользователя и передает их в защищенные средства электронной подписи и защиты информации пользователя для формирования запросов на создание и выдачу сертификата ключа проверки электронной подписи и сертификата безопасности.

19. После аутентификации с использованием единой системы идентификации и аутентификации пользователь самостоятельно осуществляет с применением защищенных средств электронной подписи и защиты информации создание ключа усиленной неквалифицированной электронной подписи, ключа проверки усиленной неквалифицированной электронной подписи и ключей для защищенных средств электронной

подписи и защиты информации, обеспечивающих возможность реализации электронного взаимодействия пользователя с автоматизированной системой по защищенным протоколам связи с использованием российских криптографических алгоритмов. С использованием защищенных средств электронной подписи и защиты информации пользователь создает запросы на создание и выдачу сертификата ключа проверки электронной подписи и сертификата безопасности, которые передаются в автоматизированную систему.

20. При положительном результате проверки соответствия данных пользователя, включенных в состав запросов на создание и выдачу сертификата ключа проверки электронной подписи и сертификата безопасности, и данных, полученных автоматизированной системой в результате аутентификации пользователя через единую систему идентификации и аутентификации, удостоверяющий центр создает сертификат ключа проверки электронной подписи пользователя, сертификат безопасности и передает их в защищенные средства электронной подписи и защиты информации пользователя, а защищенное информационное сообщение ("контейнер") сохраняет в средстве криптографической защиты информации, входящем в состав автоматизированной системы и имеющем подтверждение соответствия требованиям, установленным Федеральной службой безопасности Российской Федерации на основании модели угроз безопасности информации, указанной в пункте 13 настоящих Правил.

21. В случае изменения сведений, содержащихся в сертификате ключа проверки электронной подписи (фамилия, имя, отчество (при наличии), страховой номер индивидуального лицевого счета, идентификационный номер налогоплательщика), пользователь обязан прекратить его использование. При необходимости пользователь имеет право сформировать запрос на создание и выдачу нового сертификата ключа проверки электронной подписи.

22. Информация о выданных пользователю сертификатах ключа проверки электронной подписи, в том числе аннулированных, или действие которых досрочно прекращено, или срок действия которых истек, отображается в подсистеме "личный кабинет" пользователя на едином портале.

23. Заявление о досрочном прекращении действия сертификата ключа проверки электронной подписи может быть подано пользователем с использованием подсистемы "личный кабинет" единого портала и

подписывается усиленной квалифицированной электронной подписью, основанной на действующем квалифицированном сертификате ключа проверки электронной подписи пользователя, или простой электронной подписью, ключ которой выдан ему при личном приеме в соответствии с Правилами использования простой электронной подписи при оказании государственных и муниципальных услуг, утвержденными постановлением Правительства Российской Федерации от 25 января 2013 г. № 33 "Об использовании простой электронной подписи при оказании государственных и муниципальных услуг". Совместно с указанной простой электронной подписью на едином портале вводится короткое текстовое сообщение, направленное от единого портала на абонентский номер устройства подвижной радиотелефонной связи физического лица.

24. Пользователи обязаны соблюдать конфиденциальность ключей, созданных в их интересах в рамках настоящих Правил, а также своего пароля.

25. Использование усиленной неквалифицированной электронной подписи, созданной в соответствии с настоящими Правилами, осуществляется для подписания документов в инфраструктуре электронного правительства посредством мобильного приложения или стационарного средства вычислительной техники (при наличии технической возможности), указанных в пункте 8 настоящих Правил.

26. В мобильном приложении пользователю доступны документы от информационных систем, входящих в состав инфраструктуры электронного правительства, или информационных систем, присоединенных к инфраструктуре электронного правительства в соответствии с законодательством Российской Федерации.

27. Сертификат ключа проверки электронной подписи, выданный пользователю, содержит информацию в соответствии с требованиями Федерального закона "Об электронной подписи".

28. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации по согласованию с Федеральной службой безопасности Российской Федерации обеспечивает размещение на своем официальном сайте в информационно-телекоммуникационной сети "Интернет" сведений о содержании информации в сертификате ключа проверки электронной подписи, а также о формате сертификата ключа проверки электронной подписи.

———————