Приложение №18 к Договору присоединения № 22/2143-Д от 6 июля 2012 г.

У Т В Е Р Ж Д А Ю

Директор по информационным технологиям

АО «Гринатом»

М.П.

_____ / А.Н. Киселёв /

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ПО ИТ,
НАЧ. УПРАВЛ. И. П. ТАРАСОВ
ДОВЕРЕННОСТЬ ОТ 18.06.2021
22/306/2021-ДОВ

ПОРЯДОК

применения усиленной неквалифицированной электронной подписи

Москва 2021 г.

Содержание

1. Назначение и область применения

1.1. Настоящий Порядок применения усиленной неквалифицированной электронной подписи (далее - Порядок) разработан с целями установления порядка использования усиленной неквалифицированной электронной подписи при осуществлении электронного документооборота между участниками электронного взаимодействия в соответствии с Федеральным законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 06.04.2011г. №63-ФЗ «Об электронной подписи», другими федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, регулирующими отношения, возникающими в сфере информации, информационных технологий и защиты информации.

1.2. Порядок определяет обязательные для использования правила при использовании неквалифицированной электронной подписи при осуществлении электронного взаимодействия с помощью любой документной системы, интегрированной с Платформой доверенных сервисов Госкорпорации «Росатом».

1.3. Участник электронного взаимодействия, до начала использования неквалифицированной электронной подписи, обязан ознакомиться с данным Порядком.

1.4. Соблюдение Порядка является обязательным для предприятий/ организаций, использующих автоматизированные информационные системы, в которых применяются сертификаты ключей проверки электронных подписей, создаваемые Корпоративным удостоверяющим центром Госкорпорации «Росатом».

1.5. Ответственным за актуализацию Порядка и контроль его исполнения в соответствии с требованиями Положения о системе регламентирующих документов Госкорпорации «Росатом» является директор Департамента по информационным технологиям АО «Гринатом».

1.6. Актуальная версия Порядка размещена по адресу: https://crypto.rosatom.ru.

2. Термины, сокращения и аббревиатуры

2.1. Термины и определения

Термин	Определение
Аннулированный сертификат ключа подписи	Сертификат ключа проверки электронной подписи, действие которого прекращено в связи с: • истечением срока его действия; • получением заявления от его владельца; • вступлением в силу решения суда, влекущего аннулирование сертификата; • прекращением деятельности Удостоверяющего центра без перехода его функций другим лицам; • аннулированием неквалифицированного сертификата Удостоверяющим центром.
Владелец сертификата ключа проверки электронной подписи	Лицо, которому в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»,

	Регламентом УЦ создан сертификат ключа проверки электронной подписи.
Документная система	Корпоративная/локальная информационная система, интегрированная с Платформой доверенных сервисов Госкорпорации «Росатом», предоставляющая сервисы управления электронными документами с возможностью подписания квалифицированной/неквалифицированной электронной подписями посредством сервисов Платформы доверенных сервисов Госкорпорации «Росатом»
Неквалифицированный сертификат ключа проверки электронной подписи	Сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011г. №63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный неаккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом.
Ключ проверки электронной подписи	Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).
Ключ электронной подписи	Уникальная последовательность символов, предназначенная для создания электронной подписи.
Платформа доверенных сервисов Госкорпорации «Росатом»	Автоматизированная информационная система, предназначенная для комплексной автоматизации процессов управления ключами электронной подписи и сертификатами ключей проверки электронной подписи, предоставления сервисов удаленного подписания электронных документов, проверки электронной подписи, и сервисов управления средствами криптографической защиты информации
Регламент Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом»)	Основной руководящий документ УЦ, отражающий обязанности участников электронного взаимодействия и членов группы администраторов в части выдачи сертификата ключа проверки электронной подписи Пользователям, принятые форматы данных, а также основные организационно-технические мероприятия, необходимые для безопасного функционирования УЦ (опубликован на crypto.rosatom.ru).
Реестр удостоверяющего центра	Набор документов УЦ в электронной и/или бумажной форме, включающий следующую информацию: • реестр заявлений на регистрацию в УЦ; • реестр зарегистрированных участников электронного взаимодействия УЦ; • реестр заявок на изготовление сертификатов в УЦ; • реестр заявлений на изготовление сертификатов ключа проверки электронной подписи; • реестр заявлений на аннулирование (прекращение действия) сертификатов ключа проверки электронной подписи; • реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;

	• реестр сертификатов ключа проверки электронной подписи; • реестр изготовленных списков отозванных сертификатов ключей проверки электронной подписи.
Сертификат ключа проверки электронной подписи	Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.
Служба актуальных статусов сертификатов	Веб-сервис Удостоверяющего центра, обеспечивающий информирование Пользователей Удостоверяющего центра о статусе сертификатов ключей проверки электронной подписи посредством реализации протокола OCSP.
Служба штампов времени	Веб-сервис Удостоверяющего центра, обеспечивающий предоставление доверенных меток времени посредством реализации протокола TSP для ПДС по запросам участникам электронного взаимодействия при работе в документных системах.
Средства криптографической защиты информации	Средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче; средства имитозащиты - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации; средства электронной подписи; средства кодирования - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций; средства изготовления ключевых документов - аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств; ключевые документы - электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации

	(криптографический ключ) в шифровальных (криптографических) средствах; аппаратные шифровальные (криптографические) средства - устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин; программные шифровальные (криптографические) средства - программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств; программно-аппаратные шифровальные (криптографические) средства - устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.
Средство электронной подписи	Шифровальное (криптографическое) средство, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.
Удостоверяющий центр	Акционерное общество «Гринатом» (АО «Гринатом»), осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».
Участник электронного взаимодействия	Лицо, зарегистрированное в УЦ АО «Гринатом» в установленном Регламентом Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом») порядке, персональные данные которого указаны в сертификате ключа проверки электронной подписи.
Штамп времени электронного документа	Электронный документ, подписанный электронной подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.
Электронная подпись	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.

Электронный документ	Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.
Cryptographic Message Syntax	Стандарт, определяющий формат и синтаксис криптографических сообщений.
Online Certificate Status Protocol	Протокол установления статуса сертификата открытого ключа, реализующий RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP».
Time-Stamp Protocol	Протокол получения штампа времени, реализующий RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)».

В Порядке используются термины, установленные Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

2.2. Сокращения, используемые в целях данного документа, и расшифровки

Термин	Определение
Сертификат	Неквалифицированный сертификат ключа проверки электронной подписи
ПАК	Программно-аппаратный комплекс
ПДС	Платформа доверенных сервисов Госкорпорации «Росатом»
Регламент УЦ	Регламент Корпоративного удостоверяющего центра Госкорпорации «Росатом» (Удостоверяющего центра АО «Гринатом»)
Реестр УЦ	Реестр удостоверяющего центра
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр
ЭД	Электронный документ
ЭП	Электронная подпись
CMS	Cryptographic Message Syntax
CRL	Certificates Revocation List
OCSP	Online Certificate Status Protocol
TSP	Time-Stamp Protocol

3. Обязанности Участника электронного взаимодействия

3.1. Участник электронного взаимодействия обязан:

- следовать положениям настоящего Порядка;
- использовать ключи ЭП и соответствующие им Сертификаты для подписания/шифрования ЭД в документных системах;
- для формирования ЭП применять только действующий ключ ЭП и соответствующий ему Сертификат;
- обеспечить сохранность в тайне и защиту от несанкционированного доступа персональной аутентификационной информации для доступа к документной системе и личному ключу ЭП;

- при компрометации личной ключевой информации или аутентификационной информации немедленно прекратить ее использование, руководствоваться и соблюдать порядок выполнения действий, установленный Регламентом УЦ.

4. Удостоверяющий центр и сертификаты ключей проверки электронных подписей

4.1. Удостоверяющим центром, создающим Сертификаты для использования в документных системах, является неаккредитованный УЦ.
4.2. Для применения в документных системах могут использоваться Сертификаты, созданные только УЦ.
4.3. Порядок создания, выдачи и прекращения действия Сертификатов определяется Регламентом УЦ.
4.4. Идентификационные данные, занесенные в поле «Субъект» («Subject Name») Сертификата идентифицируют Владельца сертификата ключа проверки электронной подписи и соответствуют идентификационным данным Владельца сертификата ключа проверки электронной подписи, зарегистрированным в реестре Удостоверяющего центра.
4.5. Для определения статуса Сертификата используется список отозванных сертификатов, издаваемый и публикуемый УЦ в порядке и с периодичностью, определяемыми УЦ.
4.6. Местом публикации списков отозванных сертификатов принимается адрес информационного ресурса, определенный в расширении «Точки распространения списков отзыва (CRL)» («CRL Distribution Point») (OID – 2.5.29.31) сертификата ключа подписи.
4.7. Для определения статуса Сертификата также может использоваться Служба актуальных статусов сертификатов (в том случае, если сервис указанной Службы предоставляется Удостоверяющим центром или ПДС).

5. Средства электронной подписи

5.1. В качестве средств ЭП, обеспечивающих реализацию функций создания и проверки ЭП с использованием ключа ЭП, должны использоваться средства ЭП, имеющие подтверждение соответствия требованиям, установленным в соответствии с требованиями законодательства Российской Федерации.
5.2. Использование средства ЭП должно осуществляться в соответствии с требованиями формуляра и эксплуатационной документации на данное средство ЭП.

6. Электронные документы, подписываемые электронной подписью

6.1. Участник электронного взаимодействия вправе ЭД подписывать ЭП.
6.2. ЭД, подписанные ЭП, признаются равнозначными документам, подписанным собственноручной подписью в случае выполнения всех условий равнозначности ЭД, подписанного ЭП, документу на бумажном носителе, подписанному собственноручной подписью.

6.3. ЭД и его ЭП в документной системе представляются в виде файлов. ЭП может быть как открепленной (в виде отдельного файла), так и прикрепленной. При этом открепленная ЭП представляется в виде криптографического сообщения, формат которого определяется RFC 3852 «Cryptographic Message Syntax (CMS)», с учетом использования криптографических алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94 в соответствии с RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».
6.4. Форматы ЭД определяются документной системой.

7. Порядок формирования и проверки электронной подписи

7.1. Формирование ЭП в ЭД осуществляется в ПДС с использованием средств ЭП.
7.2. Формирование ЭП может быть осуществлено только Владельцем сертификата ключа проверки электронной подписи, соответствующий ключ ЭП которого действует на момент формирования ЭП.
7.3. При формировании ЭП:
7.3.1. с использованием сервиса ЭП на базе «КриптоПро DSS», участник электронного взаимодействия должен подтвердить свое волеизъявление на подписание ЭД с использованием OTP-via-E-Mail, либо OTP-via-push.
7.3.2. с использованием сертифицированного ФСБ России СКЗИ и отчуждаемого ключевого носителя с ключом ЭП, Участник электронного взаимодействия должен предъявить пин-код к ключевому контейнеру.
7.4. Допускается подписание одной ЭП нескольких ЭД одновременно (пакет документов) в случае таких возможностей документной системы.
7.5. ЭД может иметь несколько ЭП от нескольких различных Участников электронного взаимодействия.
7.6. При формировании ЭП в ЭД с помощью документной системы, фиксируется время подписания данного ЭД и информация о статусе Сертификата (OCSP) Владельца сертификата ключа проверки электронной подписи на момент подписания ЭД. При этом фиксация времени подписания ЭД осуществляется посредством получения метки доверенного времени (TSP).
7.7. Время, содержащееся в метке доверенного времени, полученное при подписании ЭП ЭД, признается временем подписания ЭД.
7.8. Полученная метка доверенного времени и информация о статусе Сертификата Участника электронного взаимодействия, а также иные данные, необходимые для установления статуса Сертификата на момент подписания ЭД при его хранении, обработке и передаче должны быть включены в состав криптографического сообщения и представлены в соответствии с форматом, установленным RFC 5126 «CMS Advanced Electronic Signatures (CAdES)».
7.9. Подтверждение подлинности ЭП в ЭД осуществляется с использованием сервиса по проверке Сертификатов «КриптоПро SVS», интегрируемой с ПДС.

8. Условия равнозначности электронного документа, подписанного неквалифицированной электронной подписью, документу на бумажном носителе, подписанному собственноручной подписью

8.1. Информация в электронной форме, подписанная неквалифицированной электронной подписью, признается ЭД, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания ЭД, подписанных неквалифицированной ЭП, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи.
8.1.1 Шаблон Соглашения об использовании усиленной неквалифицированной электронной подписи размещен на crypto.rosatom.ru.
Порядок проверки неквалифицированной электронной подписи:

– проверка неквалифицированных ЭП предусмотрена только для неквалифицированных ЭП, выданных ПДС;

– для проверки ЭП Участник электронного взаимодействия через интерфейс документной системы отправляет запрос в ПДС на проверку ЭП в ЭД;

– сервис проверки ЭП в ПДС осуществляет проверку действительности подписи на момент ее формирования, основываясь на достоверной информации по метке времени и статусу сертификата ключа проверки электронной подписи в момент подписания. Сертификат, относящийся к ЭП, действителен на момент подписания и его серийный номер не содержится в актуальном на указанный момент времени списке отозванных сертификатов.

– сервис проверки ЭП в ПДС осуществляет проверку целостности (неизменности) ЭД на основании сравнения хеша полученного ЭД с хешем, сформированным при подписании;

– сервис проверки ЭП в ПДС направляет ответ, содержащий информацию о результатах проверки в документную систему для предъявления участнику информационного взаимодействия.

8.2. Достоверной информацией о моменте подписания ЭД признается время, содержащееся в доверенной метке времени, полученное при подписании ЭД с использованием применяемого средства ЭП, интегрируемого с ПДС.

9. Порядок разрешения конфликтных ситуаций, связанных с применением электронной подписи

Разрешение конфликтных ситуаций осуществляется в соответствии с Регламентом УЦ.

10. Нормативные ссылки

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи";

Федеральный закон от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».