ЗАКОН КЫРГЫЗСКОЙ РЕСПУБЛИКИ

от 19 июля 2017 года № 128

Об электронной подписи

Принят Жогорку Кенешем Кыргызской Республики 15 июня 2017 года

Статья 1. Сфера действия настоящего Закона

1. Настоящий Закон регулирует отношения по использованию электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также при совершении юридически значимых действий.

2. Законами Кыргызской Республики могут устанавливаться особенности использования электронных подписей в отдельных видах отношений (подготовка и проведение выборов, совершение гражданско-правовых сделок, оказание государственных и муниципальных услуг, осуществление банковских операций, ведение бухгалтерского учета и другое).

Статья 2. Понятия, используемые в настоящем Законе

Используемые для целей настоящего Закона понятия означают следующее:

1) **электронная подпись** - информация в электронной форме, которая присоединена к другой информации в электронной форме и (или) логически связана с ней и которая используется для определения лица, от имени которого подписана информация;

2) **сертификат ключа проверки подписи** - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром и подтверждающий принадлежность ключа проверки подписи владельцу сертификата ключа проверки подписи;

3) **квалифицированный сертификат ключа проверки подписи (далее - квалифицированный сертификат)** - сертификат ключа проверки подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо органом исполнительной власти, уполномоченным в сфере использования электронной подписи, осуществляющим функции главного (корневого) удостоверяющего центра;

4) **владелец сертификата ключа проверки подписи** - лицо, которому в порядке, установленном настоящим Законом, удостоверяющим центром выдан сертификат ключа проверки подписи;

5) **ключ подписи** - уникальная последовательность символов, предназначенная для создания электронной подписи;

6) **ключ проверки подписи** - уникальная последовательность символов, однозначно связанная с ключом подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

7) **удостоверяющий центр** - юридическое лицо или индивидуальный предприниматель, осуществляющие деятельность по созданию и выдаче сертификатов ключа проверки подписи;

8) **аккредитация удостоверяющего центра** - признание органом исполнительной власти, уполномоченным в сфере использования электронной подписи, соответствия удостоверяющего центра требованиям, установленным настоящим Законом;

9) **средства электронной подписи** - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключей подписи и ключей проверки подписи;

10) **средства удостоверяющего центра** - программные и (или) аппаратные средства, используемые для реализации функций создания, хранения и выдачи сертификатов ключа проверки подписи, а также ведения реестра сертификатов ключа проверки подписи;

11) **участники электронного взаимодействия** - государственные органы, органы местного самоуправления, организации, их союзы и объединения, а также граждане, обменивающиеся информацией в электронной форме;

12) **корпоративная информационная система** - информационная система, участниками электронного взаимодействия в которой является определенный круг лиц;

13) **информационная система общего пользования** - информационная система, участниками электронного взаимодействия в которой является неопределенный круг лиц и в использовании которой этим лицам не может быть отказано;

14) **оператор информационной системы** - физическое, юридическое лицо вне зависимости от организационно-правовой формы и формы собственности, орган государственной власти, орган местного самоуправления, действующие непосредственно либо через своих представителей, осуществляющие деятельность по эксплуатации информационной системы, ее техническое и программное сопровождение.

Статья 3. Правовое регулирование отношений в области использования электронных подписей

1. Отношения в области использования электронной подписи регулируются настоящим Законом, иными законами Кыргызской Республики, в области электронного управления.

2. Порядок использования электронной подписи в корпоративной информационной системе может устанавливаться владельцем этой системы или соглашением участников электронного взаимодействия в ней, если иное не установлено законодательством Кыргызской Республики в области электронного управления.

3. Виды электронных подписей, используемых органами исполнительной власти и органами местного самоуправления, а также требования по обеспечению совместимости таких электронных подписей устанавливаются Правительством Кыргызской Республики.

Статья 4. Принципы использования электронной подписи

Принципами использования электронной подписи являются:

1) право участников электронного взаимодействия по своему усмотрению использовать любой вид электронной подписи, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено законодательными актами, иными нормативными правовыми актами (в случаях, когда законодательными актами предусмотрена такая возможность) либо соглашением участников электронного взаимодействия;

2) возможность использования участниками электронного взаимодействия по их усмотрению любой технологии и (или) технических средств, позволяющих выполнить требования настоящего Закона применительно к использованию конкретных видов электронной подписи;

3) соответствие требований к использованию конкретного вида электронной подписи, установленных в законодательных и иных нормативных правовых актах, целям, в которых используется эта электронная подпись;

4) недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на том основании, что подпись в электронном документе не является собственноручной подписью.

Статья 5. Виды электронных подписей

1. Видами электронных подписей, отношения в области использования которых регулируются настоящим Законом, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

2. Простой электронной подписью является электронная подпись, ключ подписи которой совпадает с самой электронной подписью (коды, пароли и иные идентификаторы).

3. Неквалифицированной электронной подписью является электронная подпись, которая соответствует следующим признакам:

1) электронная подпись получена в результате криптографического преобразования информации с использованием ключа подписи;

2) электронная подпись позволяет однозначно определить лицо, подписавшее электронный документ;

3) электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после его подписания;

4) электронная подпись создается с использованием средств электронной подписи, которые лицо, подписавшее электронный документ, способно сохранять под своим контролем.

4. Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Законом.

5. При использовании неквалифицированной электронной подписи сертификат ключа проверки подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Законом, может быть обеспечено без использования сертификата ключа проверки подписи.

Статья 6. Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью

1. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, за исключением случаев, когда законами или иными нормативными правовыми актами установлен запрет составления такого документа в электронной форме.

2. Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных нормативными правовыми актами или соглашением участников электронного взаимодействия, если только законами или иными нормативными правовыми актами не устанавливается запрет составления такого документа в электронной форме. Нормативные правовые акты и соглашения участников электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи.

3. Если в соответствии с законом, иными нормативными правовыми актами или обычаем делового оборота документ на бумажном носителе должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью. Нормативными правовыми актами или соглашением участников электронного взаимодействия могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.

4. Одной электронной подписью может быть подписан пакет электронных документов, то есть несколько электронных документов, связанных между собой. При подписании электронной подписью пакета электронных документов каждый из документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов.

5. Если в соответствии с законами, принимаемыми в соответствии с ними нормативными правовыми актами Кыргызской Республики, предъявляются особые требования к оформлению документов на бумажном носителе с использованием бланков строгой отчетности, то электронный документ, подписанный

квалифицированной электронной подписью, считается соответствующим этим требованиям.

Статья 7. Признание иностранных электронных подписей

1. Электронные подписи, созданные в соответствии с нормами права иностранного государства, в Кыргызской Республике признаются электронными подписями того вида, признакам которого они отвечают в соответствии с настоящим Законом.

2. Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки подписи выдан в соответствии с нормами права иностранного государства.

Статья 8. Полномочия органов исполнительной власти в сфере использования электронной подписи

1. Орган исполнительной власти, уполномоченный в сфере использования электронной подписи (далее - уполномоченный орган), и их полномочия определяются Правительством Кыргызской Республики.

2. Уполномоченный орган:

1) осуществляет аккредитацию удостоверяющих центров, в том числе осуществляет проверки соблюдения аккредитованными удостоверяющими центрами требований, на соответствие которым эти удостоверяющие центры были аккредитованы, и в случае обнаружения их несоблюдения выдает предписания об устранении нарушений;

2) осуществляет функции главного (корневого) удостоверяющего центра в отношении аккредитованных удостоверяющих центров.

3. Уполномоченный орган обязан обеспечить хранение и беспрепятственный круглосуточный доступ с применением информационно-телекоммуникационных сетей к следующей информации:

1) наименования, адреса аккредитованных удостоверяющих центров;

2) реестр выданных и аннулированных уполномоченным органом, осуществляющим функции главного (корневого) удостоверяющего центра, квалифицированных сертификатов;

3) перечень удостоверяющих центров, аккредитация которых аннулирована;

4) перечень аккредитованных центров, аккредитация которых приостановлена;

5) перечень аккредитованных удостоверяющих центров, деятельность которых прекращена;

6) реестры сертификатов, переданные уполномоченному органу в соответствии со статьей 15 настоящего Закона.

4. Правительство Кыргызской Республики устанавливает:

1) порядок передачи реестров и иной информации в уполномоченный орган в случае прекращения деятельности аккредитованного удостоверяющего центра;

2) порядок формирования и ведения реестров квалифицированных сертификатов, а также предоставления сведений из таких реестров;

3) правила аккредитации удостоверяющих центров, в том числе порядок проверки соблюдения аккредитованными удостоверяющими центрами требований, на соответствие которым эти удостоверяющие центры были аккредитованы.

5. Орган исполнительной власти в области обеспечения безопасности:

1) устанавливает требования к форме квалифицированного сертификата;

2) устанавливает требования к средствам электронной подписи и средствам удостоверяющего центра;

3) осуществляет подтверждение соответствия средств электронной подписи и средств удостоверяющего центра требованиям, установленным в соответствии с настоящим Законом, и публикует перечень таких средств.

Статья 9. Использование простой электронной подписи

1. Электронный документ считается подписанным простой электронной подписью при выполнении одного из следующих условий:

1) простая электронная подпись содержится в самом электронном документе;

2) указание ключа простой электронной подписи в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляется создание и (или) отправка электронного документа, было необходимым условием создания и (или) отправки электронного документа с использованием такой информационной системы, и в созданном (отправленном) электронном документе содержится информация, однозначно указывающая на лицо, от имени которого был создан (отправлен) электронный документ.

2. При использовании простой электронной подписи не применяются ключ проверки подписи, средства электронной подписи и сертификат ключа проверки подписи.

3. Случаи и порядок использования простой электронной подписи устанавливаются нормативными правовыми актами и (или) соглашениями участников электронного взаимодействия, предусматривающими равнозначность электронных документов, подписанных простой электронной подписью, документам на бумажном носителе, подписанным собственноручной подписью. Такие акты и соглашения должны предусматривать, в частности:

1) механизм определения лица, от имени которого подписан электронный документ, по его простой электронной подписи;

2) обязанность соблюдать конфиденциальность ключа простой электронной подписи.

4. К созданию, выдаче и использованию простой электронной подписи не применяются правила, установленные для усиленной электронной подписи.

5. Использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, а также для создания электронных документов, требующих нотариального удостоверения или государственной регистрации в соответствии с законодательством Кыргызской Республики, не допускается.

Статья 10. Обязанности участников электронного взаимодействия при использовании усиленной электронной подписи

При использовании усиленной электронной подписи участники электронного взаимодействия обязаны:

1) обеспечивать конфиденциальность ключа подписи, в частности, не допускать использование принадлежащих им ключей подписи без их согласия;

2) незамедлительно, но в любом случае в течение не более чем одного рабочего дня с момента получения информации о нарушении конфиденциальности ключа подписи, уведомлять удостоверяющий центр, выдавший сертификат ключа проверки подписи, и иных участников электронного взаимодействия о таком нарушении;

3) при наличии оснований полагать, что конфиденциальность ключа подписи нарушена, не использовать данный ключ;

4) использовать средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Законом, для осуществления обмена электронными документами, подписанными квалифицированной электронной подписью.

Статья 11. Признание подлинности квалифицированной электронной подписи

До тех пор, пока решением суда не установлено иное, квалифицированная подпись признается подлинной при одновременном соблюдении следующих условий:

1) квалифицированный сертификат, содержащий ключ проверки подписи, создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна (не приостановлена, не прекращена, не аннулирована) на день выдачи указанного сертификата;

2) квалифицированный сертификат, содержащий ключ проверки подписи, действителен (не прекратил свое действие, не аннулирован) на день подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки - если момент подписания не определен;

3) имеется положительный результат проверки принадлежности владельцу указанного сертификата квалифицированной электронной подписи, с помощью которой подписан данный электронный документ, и отсутствия изменений, внесенных в этот документ, после его подписания. При этом проверка осуществляется с применением средств электронной подписи, получивших подтверждение соответствия требованиям, установленным в соответствии с настоящим Законом, и с использованием квалифицированного сертификата лица, от имени которого подписан документ;

4) квалифицированная электронная подпись используется в соответствии с ограничениями, содержащимися в квалифицированном сертификате лица, от имени которого подписан данный документ (если ограничения установлены).

Статья 12. Средства электронной подписи

1. Для создания и проверки электронной подписи, создания ключей подписи и ключей проверки подписи должны использоваться средства электронной подписи, которые:

1) позволяют установить факт изменения подписанного электронного документа после его подписания;

2) обеспечивают практическую невозможность вычисления ключа подписи из электронной подписи или из ключа ее проверки.

2. При создании электронной подписи средство электронной подписи должно:

1) показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

2) создавать электронную подпись лишь после подтверждения лицом, подписывающим информацию, операции по созданию электронной подписи;

3) однозначно и ясно показывать, что электронная подпись создана.

3. При проверке электронной подписи средство электронной подписи должно:

1) показывать содержание электронного документа, подписанного электронной подписью;

2) показывать, вносились ли изменения в подписанный электронной подписью электронный документ;

3) указывать на лицо, с использованием ключа подписи которого подписаны электронные документы.

4. Средства электронной подписи, предназначенные для создания электронной подписи в электронных документах, содержащих сведения, составляющие государственные секреты, или предназначенные для использования в информационной системе, содержащей государственные секреты, подлежат обязательной сертификации на соответствие требованиям по защите сведений соответствующей степени секретности.

Средства электронной подписи, предназначенные для создания электронной подписи в электронных документах, содержащих конфиденциальную информацию, не должны нарушать конфиденциальности такой информации.

5. Требования частей 2 и 3 настоящей статьи не применяются к средствам электронной подписи, используемым для автоматического создания или проверки электронных подписей в информационной системе.

Статья 13. Удостоверяющий центр

1. Удостоверяющий центр:

1) создает сертификат ключа проверки подписи и выдает его лицу, обратившемуся за получением такого сертификата (далее - заявитель);

2) устанавливает сроки действия сертификатов ключа проверки подписи;

3) аннулирует выданные им сертификаты ключа проверки подписи;

4) по обращению заявителя выдает средства электронной подписи, содержащие ключ подписи и ключ проверки подписи (в том числе созданные удостоверяющим центром) либо обеспечивающие возможность создания ключа подписи и ключа проверки подписи заявителем;

5) ведет реестр выданных и аннулированных им сертификатов ключа проверки подписи (далее - реестр сертификатов), включающий в том числе сведения, содержащиеся в выданных им сертификатах ключа проверки подписи, а также сведения о дате прекращения действия (аннулирования) сертификата ключа проверки подписи и его основании;

6) устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц

к информации, содержащейся в реестре сертификатов, в том числе с использованием Интернета;

7) по обращению заявителей создает ключи подписи и ключи проверки подписи.

В случае создания им ключей подписи удостоверяющий центр обеспечивает конфиденциальность таких ключей;

8) проверяет уникальность ключей проверки подписи в реестре сертификатов данного удостоверяющего центра;

9) осуществляет по обращениям участников электронного взаимодействия проверку электронной подписи;

10) осуществляет иную деятельность, связанную с использованием электронной подписи.

2. Удостоверяющий центр обязан:

1) информировать заявителей в письменной форме об условиях и порядке использования электронной подписи и средств электронной подписи, о рисках, связанных с использованием электронной подписи, и мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

2) обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, а также от иных неправомерных действий в отношении такой информации;

3) безвозмездно предоставлять любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов сведения, содержащиеся в реестре сертификатов удостоверяющего центра, в том числе информацию об аннулировании сертификата ключа проверки подписи.

3. Удостоверяющий центр в соответствии с законодательством Кыргызской Республики несет ответственность за вред, причиненный иным лицам в результате:

1) неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг удостоверяющим центром;

2) неисполнения или ненадлежащего исполнения обязанностей, предусмотренных пунктом 9 части 1, пунктами 2 и 3 части 2 настоящей статьи.

4. Удостоверяющий центр вправе наделить иных лиц (далее - доверенные лица) полномочиями по созданию и выдаче сертификатов ключа проверки подписи от имени удостоверяющего центра, подписываемых электронной подписью, основанной на сертификате ключа проверки подписи, выданного такому доверенному лицу этим удостоверяющим центром.

5. Удостоверяющий центр, указанный в части 4 настоящей статьи, является главным (корневым) удостоверяющим центром по отношению к доверенным лицам и выполняет по отношению к ним следующие функции:

1) осуществляет проверку электронных подписей, ключи проверки подписи которых указаны в сертификатах ключей проверки подписи, выданных доверенными лицами;

2) обеспечивает электронное взаимодействие между доверенными лицами и доверенных лиц с удостоверяющим центром.

6. Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности удостоверяющего центра, если более короткий

срок не установлен нормативными правовыми актами. В случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам он должен заблаговременно, но не менее чем за один месяц до даты прекращения деятельности, уведомить об этом в письменной форме владельцев выданных им сертификатов ключа проверки подписи, срок действия которых не истек. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть уничтожена.

В случае прекращения деятельности удостоверяющего центра с переходом его функций другим лицам он должен заблаговременно, но не менее чем за один месяц до даты передачи своих функций, уведомить об этом в письменной форме владельцев выданных им сертификатов ключа проверки подписи, срок действия которых не истек. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть передана лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность.

7. Порядок реализации функций удостоверяющего центра, осуществления его прав и исполнения обязанностей, установленных настоящей статьей, определяется удостоверяющим центром самостоятельно, если иное не установлено нормативным правовым актом или соглашением участников электронного взаимодействия.

8. Договор на оказание услуг удостоверяющим центром, реализующим свою деятельность в отношении неограниченного круга лиц с использованием информационной системы общего пользования, является публичным договором.

Статья 14. Сертификат ключа проверки подписи

1. Удостоверяющий центр осуществляет создание и выдачу сертификата ключа проверки подписи на основании соглашения между удостоверяющим центром и заявителем.

2. Сертификат ключа проверки подписи должен содержать следующие сведения:

1) даты начала и окончания срока его действия;

2) фамилию, имя, отчество (если имеется) - для физических лиц (наименование - для юридических лиц) или иной идентификатор владельца сертификата ключа проверки подписи;

3) ключ проверки подписи;

4) наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ подписи и ключ проверки подписи;

5) наименование удостоверяющего центра, который выдал сертификат.

3. В случае выдачи сертификата ключа проверки подписи юридическому лицу в качестве владельца сертификата ключа проверки подписи, наряду с указанием юридического лица, указывается физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности. Допускается не указывать в качестве владельца сертификата ключа проверки подписи физическое лицо, действующее от имени юридического лица, в сертификатах ключа проверки подписи, используемых для автоматического создания или проверки электронных подписей в информационной системе.

Владельцем такого сертификата ключа проверки подписи признается юридическое лицо, указанное в данном сертификате.

4. Удостоверяющий центр вправе выдавать сертификаты ключа проверки подписи как в форме электронного документа, так и в форме документа на бумажном носителе. Владелец сертификата ключа проверки подписи, выданного в форме электронного документа, вправе также получить копию сертификата ключа проверки подписи на бумажном носителе, заверенную удостоверяющим центром.

5. Сертификат ключа проверки подписи действует с момента его выдачи, если иная дата начала действия сертификата ключа проверки подписи не указана в самом сертификате ключа проверки подписи.

Сведения о сертификате ключа проверки подписи должны быть внесены удостоверяющим центром в реестр сертификатов не позднее даты начала действия сертификата ключа проверки подписи, указанной в нем.

6. Сертификат ключа проверки подписи прекращает свое действие:

1) по истечении установленного в нем срока его действия;

2) по заявлению владельца сертификата ключа проверки подписи, подаваемому в форме документа на бумажном носителе либо в электронной форме;

3) в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;

4) в иных случаях, установленных законом или соглашением удостоверяющего центра с владельцем сертификата ключа проверки подписи.

7. Информация о прекращении действия сертификата ключа проверки подписи должна быть внесена удостоверяющим центром в реестр сертификатов в течение одного рабочего дня с момента, когда удостоверяющему центру стало известно о наступлении обстоятельств, повлекших прекращение действие сертификата ключа проверки подписи. Сертификат ключа проверки подписи прекращает свое действие с момента внесения записи об этом в реестр сертификатов.

8. Удостоверяющий центр незамедлительно, но не более чем в течение одного рабочего дня, аннулирует сертификат ключа проверки подписи путем внесения записи об аннулировании в реестр сертификатов по решению суда, вступившему в законную силу, в частности в случае, если решением суда установлено, что сертификат ключа проверки подписи содержит недостоверные данные.

9. Использование аннулированного сертификата ключа проверки подписи не влечет юридических последствий, за исключением тех, которые связаны с его аннулированием.

Удостоверяющий центр обязан до внесения в реестр сертификатов сведений об аннулировании сертификата ключа проверки подписи уведомить владельца сертификата ключа проверки подписи в письменной форме об аннулировании его сертификата ключа проверки подписи.

Статья 15. Аккредитованный удостоверяющий центр

1. Удостоверяющий центр, получивший аккредитацию, является аккредитованным удостоверяющим центром.

2. Аккредитованный удостоверяющий центр обязан хранить следующие сведения:

1) реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;

2) сведения о наименовании, номере и дате выдачи документа, подтверждающего права лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;

3) сведения о наименовании, номере и дате выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если сведения о полномочиях владельца квалифицированного сертификата действовать по поручению третьих лиц включены в квалифицированный сертификат.

3. Указанная информация должна храниться аккредитованным удостоверяющим центром в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Кыргызской Республики.

Информация должна храниться в форме, позволяющей проверить ее целостность и достоверность.

Удостоверяющий центр должен обеспечивать владельцу квалифицированного сертификата доступ к информации, относящейся к владельцу квалифицированного сертификата и хранимой в аккредитованном удостоверяющем центре.

4. В случае прекращения деятельности аккредитованного удостоверяющего центра он обязан:

1) сообщить об этом уполномоченному органу не позднее чем за один месяц до даты прекращения деятельности удостоверяющего центра;

2) передать уполномоченному органу в установленном порядке реестр сертификатов;

3) передать на хранение уполномоченному органу в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

Статья 16. Аккредитация удостоверяющего центра

1. Аккредитация удостоверяющего центра осуществляется уполномоченным органом в отношении удостоверяющих центров, являющихся юридическими лицами.

2. Аккредитация удостоверяющего центра осуществляется на добровольной основе.

Аккредитация удостоверяющего центра осуществляется на пятилетний срок, если меньший срок не указан в заявлении удостоверяющего центра.

3. Аккредитация предоставляется при условии выполнения удостоверяющим центром следующих требований:

1) стоимость чистых активов удостоверяющего центра составляет не менее одного миллиона сомов;

2) наличие финансового обеспечения ответственности за убытки, причиненные иным лицам вследствие их доверия к сведениям, указанным в сертификате ключа проверки подписи, выданном таким удостоверяющим центром, или информации, содержащейся в реестре сертификатов данного удостоверяющего центра, в сумме не менее полутора миллионов сомов;

3) наличие средств электронной подписи и средств удостоверяющего центра, получивших подтверждение соответствия требованиям, установленным органом исполнительной власти в области обеспечения безопасности;

4) наличие в штате удостоверяющего центра не менее 2 сотрудников, непосредственно осуществляющих деятельность по созданию и выдаче сертификатов ключа проверки подписи, имеющих высшее профессиональное образование в области информационных технологий или информационной безопасности либо высшее или среднее профессиональное образование и прошедших переподготовку или повышение квалификации по вопросам использования электронной подписи.

4. Аккредитация удостоверяющего центра осуществляется по его заявлению, подаваемому в уполномоченный орган.

К заявлению прилагаются документы, подтверждающие соответствие удостоверяющего центра требованиям, установленным частью 3 настоящей статьи.

5. Уполномоченный орган на основании представленных документов в срок, не превышающий 30 календарных дней, принимает решение об аккредитации удостоверяющего центра или об отказе в аккредитации.

В случае принятия решения об аккредитации удостоверяющего центра уполномоченный орган в срок, не превышающий 10 дней с момента принятия решения об аккредитации, уведомляет удостоверяющий центр о принятом решении и выдает свидетельство об аккредитации по установленной форме. Одновременно с выдачей свидетельства об аккредитации уполномоченным органом, осуществляющим функции главного (корневого) удостоверяющего центра, аккредитованному удостоверяющему центру выдается квалифицированный сертификат, созданный с использованием средств указанного главного (корневого) удостоверяющего центра.

В случае принятия решения об отказе в аккредитации удостоверяющего центра уполномоченный орган в срок, не превышающий десяти календарных дней с момента принятия решения об отказе в аккредитации, направляет или вручает удостоверяющему центру письменное уведомление о принятом решении с указанием причин отказа.

6. Основанием для отказа в аккредитации является несоответствие удостоверяющего центра требованиям, установленным частью 3 настоящей статьи, либо наличие в представленных документах недостоверной информации.

7. Аккредитованный удостоверяющий центр должен соблюдать требования, на соответствие которым он аккредитован, в течение всего срока его аккредитации. В случае возникновения обстоятельств, делающих невозможным их соблюдение, удостоверяющий центр должен немедленно уведомить об этом в письменной форме уполномоченный орган.

Аккредитованный удостоверяющий центр при осуществлении своих функций и исполнении принятых обязательств должен соблюдать требования, установленные для удостоверяющих центров настоящим Законом.

Уполномоченный орган в течение всего срока аккредитации обязан проводить проверки соблюдения аккредитованными удостоверяющими центрами требований, установленных настоящим Законом.

В случае обнаружения несоблюдения аккредитованным удостоверяющим центром указанных требований уполномоченный орган обязан выдать

удостоверяющему центру предписание об устранении нарушений с установлением срока их устранения и приостановить действие аккредитации на указанный срок с внесением сведений об этом в перечень, утверждаемый уполномоченным органом. Аккредитованный удостоверяющий центр письменно уведомляет уполномоченный орган об устранении нарушений, послуживших основанием для приостановления его аккредитации. Уполномоченный орган вправе проверить фактическое устранение нарушений, после чего принимает решение о возобновлении действия аккредитации, а при их неустранении в указанный в предписании срок - аннулирует аккредитацию удостоверяющего центра.

8. На государственные органы, органы местного самоуправления, государственные и муниципальные учреждения, осуществляющие функции удостоверяющего центра, не распространяются требования, установленные пунктами 1 и 2 части 3 настоящей статьи.

9. Главный (корневой) удостоверяющий центр, функции которого осуществляет уполномоченный орган, не подлежит аккредитации в соответствии с настоящим Законом.

Статья 17. Квалифицированный сертификат

1. Квалифицированный сертификат подлежит созданию с использованием средств удостоверяющего центра, получивших подтверждение соответствия требованиям, установленным в соответствии с настоящим Законом.

2. Квалифицированный сертификат должен содержать следующие сведения:

1) уникальный номер квалифицированного сертификата, даты начала и окончания его действия;

2) фамилию, имя и отчество (если имеется), дату и место рождения владельца квалифицированного сертификата - физического лица либо наименование (фирменное наименование), регистрационный номер и место регистрации и (или) фактического нахождения исполнительного органа владельца квалифицированного сертификата - юридического лица;

3) ключ проверки подписи;

4) наименование средств электронной подписи и средств удостоверяющего центра, которые использованы для создания ключа подписи, ключа проверки подписи и квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с настоящим Законом;

5) наименование и местонахождение удостоверяющего центра, который выдал квалифицированный сертификат, номер квалифицированного сертификата удостоверяющего центра и реквизиты свидетельства об аккредитации этого центра;

6) ограничения использования квалифицированного сертификата (если ограничения устанавливаются);

7) иные сведения о заявителе (по требованию заявителя).

3. Если заявителем представлены в удостоверяющий центр документы, подтверждающие его право действовать от имени третьих лиц, в квалифицированный сертификат включаются сведения, свидетельствующие о таких правомочиях заявителя и сроке действия указанных правомочий.

4. Квалифицированный сертификат выдается в форме, требования к которой устанавливаются органом исполнительной власти в области обеспечения безопасности.

5. В случае аннулирования квалифицированного сертификата, выданного аккредитованному удостоверяющему центру, который выдал квалифицированный сертификат заявителю, а также в случае аннулирования или истечения срока аккредитации удостоверяющего центра квалифицированный сертификат, выданный аккредитованным удостоверяющим центром заявителю, прекращает свое действие.

6. Владелец квалифицированного сертификата обязан:

1) при наличии оснований полагать, что конфиденциальность ключа подписи нарушена, не использовать данный ключ и немедленно обратиться в удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения действия этого сертификата;

2) использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если такие ограничения установлены).

Статья 18. Выдача квалифицированного сертификата

1. Аккредитованный удостоверяющий центр при выдаче квалифицированного сертификата обязан:

1) установить личность заявителя - физического лица, обратившегося к нему за получением квалифицированного сертификата;

2) получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата.

2. Заявитель при обращении в удостоверяющий центр указывает на ограничения использования квалифицированного сертификата (в случаях когда ограничения устанавливаются), а также представляет удостоверяющему центру следующие документы, подтверждающие достоверность сведений, предоставленных заявителем для включения в квалифицированный сертификат, либо их надлежащим образом нотариально заверенные копии:

1) основной документ, удостоверяющий личность заявителя - физического лица, или учредительные документы и свидетельство о государственной регистрации заявителя - юридического лица;

2) надлежащим образом заверенный перевод на государственный или официальный язык документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц);

3) доверенность или иной документ, подтверждающие право заявителя действовать от имени других лиц.

3. При получении квалифицированного сертификата заявитель под расписку должен быть ознакомлен удостоверяющим центром со сведениями, содержащимися в квалифицированном сертификате.

4. Удостоверяющий центр одновременно с выдачей квалифицированного сертификата должен выдать владельцу квалифицированного сертификата

руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Статья 19. Заключительные и переходные положения

1. Сертификаты ключей подписи, выданные в соответствии с Законом Кыргызской Республики "Об электронном документе и электронной цифровой подписи", признаются сертификатами ключей проверки подписи в соответствии с настоящим Законом и продолжают действовать до истечения указанного в них срока по правилам, установленным настоящим Законом для квалифицированных сертификатов.

2. Электронный документ, подписанный электронной цифровой подписью, как она определена Законом Кыргызской Республики "Об электронном документе и электронной цифровой подписи", до даты вступления в силу настоящего Закона признается электронным документом, подписанным квалифицированной электронной подписью, пока иное не будет установлено решением суда.

Статья 20. Вступление в силу настоящего Закона

1. Настоящий Закон вступает в силу по истечении пятнадцати дней со дня официального опубликования.

Опубликован в газете "Эркин Тоо" от 25 июля 2017 года № 84-85 (2809-2810)

2. Признать утратившим силу Закон Кыргызской Республики "Об электронном документе и электронной цифровой подписи" от 17 июля 2004 года № 92.

3. Правительству Кыргызской Республики привести свои нормативные правовые акты в соответствие с настоящим Законом.

Президент
Кыргызской Республики **А.Ш. Атамбаев**