107
Перевод

ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ МОЛДОВА

ПОСТАНОВЛЕНИЕ № 203

от 30 марта 2022 г.

Кишинэу

О проекте закона об электронной идентификации и доверительных услугах

Правительство ПОСТАНОВЛЯЕТ:

Одобрить и представить Парламенту на рассмотрение проект закона об электронной идентификации и доверительных услугах.

Премьер-министр **НАТАЛЬЯ ГАВРИЛИЦА**

Контрасигнует:

Министр юстиции Серджиу Литвиненко

Проект
Перевод
ЕС

ПАРЛАМЕНТ РЕСПУБЛИКИ МОЛДОВА

ЗАКОН
об электронной идентификации и доверительных услугах

Парламент принимает настоящий органический закон.

Данный закон частично перекладывает Регламент (ЕС) № 910/2014 Европейского парламента и Совета от 23 июля 2014 года об электронной идентификации и доверительных услугах для электронных сделок на внутреннем рынке и отменяет Директиву 1999/93/ЕС, опубликованный в Официальном журнале Европейского союза L 257 от 28 августа 2014 года.

Глава I
ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Цель и сфера применения настоящего закона

(1) Настоящий закон направлен на обеспечение надлежащего функционирования национального рынка в области безопасности электронных средств идентификации и доверительных услуг и устанавливает правовые основы для электронных подписей, электронных печатей, электронных штампов времени, электронных документов, зарегистрированных услуг электронного распространения и сертификационных услуг для аутентификации веб-страниц.

(2) Настоящий закон не ограничивает использование документов.

Статья 2. Основные понятия

Для целей настоящего закона используются следующие понятия:

аутентификация – электронный процесс, позволяющий подтвердить электронную идентификацию физического или юридического лица или происхождение и целостность данных в электронной форме;

защищенный электронный архив – структурированное хранилище электронных документов, которое обеспечивает их конфиденциальность, неотрекаемость и целостность и гарантирует доказательную ценность электронных документов с течением времени;

сертификат открытого ключа – электронный документ, содержащий открытый ключ, на который нанесена электронная подпись или электронная печать поставщика доверительных услуг,

удостоверяющий, что ключ принадлежит владельцу сертификата открытого ключа, и позволяющий идентифицировать этого владельца;

квалифицированный сертификат открытого ключа – сертификат открытого ключа, удовлетворяющий требованиям, предусмотренным статьей 13, и выдан поставщиком доверительных услуг, удовлетворяющий требованиям, предусмотренным статьей 8;

сертификат электронной подписи – электронное удостоверение, связывающее данные проверки электронной подписи с физическим лицом и подтверждающее, как минимум, имя этого лица;

сертификат электронной печати – электронное удостоверение, связывающее данные проверки электронной печати с юридическим лицом и подтверждающее наименование этого лица;

квалифицированный сертификат электронной подписи – означает сертификат электронной подписи, который выдан квалифицированным поставщиком доверительных услуг и который удовлетворяет требованиям, предусмотренным статьей 25;

квалифицированный сертификат для электронной печати – означает сертификат для электронной печати, который выдается квалифицированным поставщиком доверительных услуг и который удовлетворяет требованиям, предусмотренным статьей 25;

создатель печати – юридическое лицо, создающее электронную печать;

сертификат для аутентификации веб-страницы – сертификат, позволяющий аутентифицировать веб-страницу и связывающий веб-страницу с физическим или юридическим лицом, которому выдан сертификат;

квалифицированный сертификат для аутентификации веб-страницы – сертификат для аутентификации веб-страницы, выданный квалифицированным поставщиком доверительных услуг и удовлетворяющий требованиям, предусмотренным статьей 34;

открытый ключ – уникальная цифровая последовательность, сформированная с помощью устройства создания электронной подписи или электронной печати, соответствующая связанному с ним закрытому ключу и предназначенная для использования при проверке подлинности электронной подписи;

закрытый ключ – уникальный цифровой последовательный ключ, сформированный с помощью устройства создания электронной подписи или электронной печати и предназначенный для использования при создании электронной подписи или электронной печати;

персональные идентификационные данные – совокупность данных, позволяющих установить личность физического или юридического лица или физического лица, представляющего юридическое лицо;

данные для создания электронной подписи или электронной печати – уникальные данные, которые используются лицом, подписавшим или создавшим печать, для создания электронной подписи или электронной печати;

данные проверки – данные, которые используются для проверки электронной подписи или электронной печати;

данные проверки электронной подписи или электронной печати – данные, которые используются в целях проверки электронной подписи или электронной печати;

устройство создания электронной подписи или электронной печати – сконфигурированное программное или аппаратное обеспечение, используемое для создания электронной подписи или печати;

квалифицированное устройство для создания электронной подписи или электронной печати – устройство для создания электронной подписи или электронной печати, удовлетворяющее требованиям, предусмотренным статьей 27;

устройство пróверки электронной подписи или электронной печати – сконфигурированное программное или аппаратное обеспечение, используемое для реализации данных проверки электронной подписи или электронной печати;

электронный документ – любое содержание в электронной форме, в частности в форме текста или звуковой, визуальной или аудиовизуальной записи, к которому прикреплена электронная подпись или электронная печать;

электронная идентификация – процесс использования персональных идентификационных данных в электронной форме, однозначно представляющих физическое или юридическое лицо или физическое лицо, представляющее юридическое лицо;

посредник электронного документа – индивидуальный предприниматель или юридическое лицо, которое от имени подписанта или создателя печати и/или получателя электронного документа организует и администрирует систему электронного документооборота и/или оказывает услуги, связанные с электронным документооборотом;

электронное средство идентификации – материальная или нематериальная единица, содержащая персонально идентифицируемые данные, которые используются для аутентификации в рамках онлайн-сервиса;

электронная временная метка – данные в электронной форме, которые связывают другие данные в электронной форме с определенным моментом времени, устанавливая доказательство того, что последние существовали в то время;

квалифицированная электронная временная метка – означает электронную временную метку, удовлетворяющую требованиям, предусмотренным статьей 31;

поставщик доверительных услуг – индивидуальный предприниматель или юридическое лицо, предоставляющее одну или несколько доверительных услуг в качестве квалифицированного или неквалифицированного поставщика доверительных услуг;

квалифицированный поставщик доверительных услуг – поставщик доверительных услуг, который предоставляет одну или несколько квалифицированных доверительных услуг и которому орган надзора и контроля присвоил квалифицированный статус;

продукт – аппаратное и/или программное обеспечение или их отдельные компоненты, предназначенные для использования при оказании доверительных услуг;

электронная подпись – данные в электронной форме, которые прикреплены к другим данным в электронной форме или логически связаны с ними и используются в качестве метода аутентификации;

усиленная электронная подпись – электронная подпись, удовлетворяющая требованиям, предусмотренным статьей 23;

квалифицированная электронная подпись – усиленная электронная подпись, которая создается с помощью устройства создания квалифицированной электронной подписи и основывается на сертификате квалифицированной электронной подписи;

подписант – физическое лицо, создающее электронную подпись;

доверительная услуга – электронная услуга, обычно предоставляемая за вознаграждение, состоящая из одного или нескольких действий, перечисленных ниже:

a) создание, проверка и подтверждение электронных подписей, электронных печатей или электронных штампов времени, зарегистрированных услуг электронного распространения и сертификатов, связанных с этими услугами;

b) создание, проверка и подтверждение сертификатов для аутентификации веб-страницы;

c) обслуживание электронных подписей, печатей или сертификатов, связанных с этими услугами;

квалифицированная доверительная служба – доверительная служба, которая отвечает требованиям, изложенным в настоящем Законе;

электронная печать – данные в электронной форме, прикрепленные или логически связанные с другими данными в электронной форме для обеспечения происхождения и целостности последних;

усиленная электронная печать – электронная печать, удовлетворяющая требованиям, предусмотренным статьей 23;

квалифицированная электронная печать – усиленная электронная печать, которая создается создателем квалифицированной электронной печати и основывается на сертификате квалифицированной электронной печати;

зарегистрированная служба электронной доставки – служба, которая позволяет передавать данные между третьими лицами с помощью электронных средств и предоставляет доказательства обработки переданных данных, включая доказательства передачи и получения данных, а также защищает переданные данные от риска потери, кражи, повреждения или любого несанкционированного изменения;

квалифицированная зарегистрированная служба электронной доставки – зарегистрированная служба электронной доставки, удовлетворяющая требованиям, предусмотренным статьей 33;

владелец сертификата открытого ключа – физическое или юридическое лицо или физическое лицо, представляющее юридическое лицо, которое пользуется доверительными услугами;

орган надзора и контроля – центральный орган государственной власти, созданный в соответствии с настоящим законом, наделенный полномочиями по надзору и контролю в области электронной идентификации и доверительных услуг;

валидация – процесс проверки и подтверждения того, что электронная подпись или электронная печать действительна.

Статья 3. Взаимное признание

(1) Признание сертификатов открытых ключей за пределами Республики Молдова регулируется международными договорами, стороной которых является Республика Молдова. Если международные договоры, стороной которых является Республика Молдова, устанавливают иные правила, чем те, которые предусмотрены настоящим Законом, применяются правила международных договоров.

(2) Сертификат открытого ключа, выданный поставщиком доверительных услуг, зарегистрированным или учрежденным в другом государстве, признается эквивалентным, с точки зрения юридических последствий, сертификату открытого ключа, выданному поставщиком доверительных услуг, зарегистрированным или учрежденным в Республике Молдова, если выполняется одно из следующих условий:

a) поставщик доверительных услуг, домицилированный или учрежденный в другом государстве, был аккредитован в рамках схемы аккредитации в соответствии с положениями настоящего Закона;

b) квалифицированный поставщик доверительных услуг, домицилированный или учрежденный в Республике Молдова, гарантирует признание сертификата;

c) сертификат или выдавший его поставщик доверительных услуг признан посредством применения двустороннего или многостороннего соглашения между Республикой Молдова и другими государствами или международными организациями на основе взаимности.

(3) Доверительные услуги и электронные документы не могут считаться лишенными юридической силы только на основании того, что сертификат открытого ключа был выдан в соответствии с правилами иностранного государства, если он был признан на условиях, указанных в пункте (2) статьи 3.

(4) В отступление от положений пунктов (1) и (2) статьи 3 квалифицированный сертификат открытого ключа, выданный поставщиком доверительных услуг государства-члена Европейского Союза, признается эквивалентным, с точки зрения его юридической силы, сертификату открытого ключа, выданному поставщиком доверительных услуг, домицилированным или учрежденным в Республике Молдова..

(5) Порядок признания квалифицированного сертификата открытого ключа, выданного поставщиком услуг доверия в государстве-члене Европейского союза, определяется Правительством.

(6) Устройство проверки электронной подписи или электронной печати, используемое для проверки электронной подписи или электронной печати по смыслу пункта (4) статьи 3, должно иметь подтверждение соответствия требованиям настоящего закона, выданное компетентным органом.

Глава II
ЭЛЕКТРОННАЯ ИДЕНТИФИКАЦИЯ И ДОВЕРИТЕЛЬНЫЕ УСЛУГИ

Раздел 1
Общая информация об электронной идентификации и доверительных услугах

Статья 4. Доступность для людей с ограниченными возможностями

По возможности, предоставляемые доверительные услуги и продукты конечного пользователя, используемые для предоставления этих услуг, должны быть доступны для людей с ограниченными возможностями.

Статья 5. Идентификация лиц в информационных системах

(1) Идентификация лиц в информационных системах не может быть ограничена идентификационными или другими идентифицирующими данными.

(2) Если идентификация запрашивается с использованием квалифицированных доверительных услуг, должны использоваться

квалифицированные доверительные услуги, предусмотренные настоящим Законом.

Статья 6. Поставщик доверительных услуг

(1) Поставщики доверительных услуг могут быть квалифицированными или неквалифицированными.

(2) Поставщики доверительных услуг организованы по иерархическому принципу. На вершине иерархии находится поставщик доверительных услуг высшего уровня.

(3) Неквалифицированные поставщики доверительных услуг должны организовать свою иерархию самостоятельно.

(4) Деятельность квалифицированных поставщиков доверительных услуг, включая их иерархию, должна быть организована в порядке, определенным Правительством, в соответствии с положениями настоящего Закона.

(5) Записи о квалифицированных поставщиках доверительных услуг хранятся органом надзора и контроля в Регистре записей о квалифицированных поставщиках доверительных услуг, который постоянно обновляется и доступ к которому является открытым.

(6) Внесение в регистр квалифицированных поставщиков доверительных услуг осуществляется органом надзора и контроля в день их аккредитации.

Статья 7. Заявка на аккредитацию

(1) Для целей аккредитации поставщик доверительных услуг должен представить следующие документы:

a) заявление на аккредитацию в соответствии с образцом, установленным органом надзора и контроля;

b) банковская гарантия или страховой полис на сумму 300 000 леев;

c) регламент работы поставщика доверительных услуг;

d) копия приказа о назначении сотрудников поставщика доверительных услуг и лиц, уполномоченных подписывать сертификаты открытых ключей, а также копия документов, удостоверяющих их личность;

e) копия документов, подтверждающих образование и квалификацию лиц, занимающих ответственные должности и участвующих в предоставлении услуг по сертификации;

f) план расположения помещений и порядок доступа в специальные помещения;

g) акт, регламентирующий хранение резервных копий реестра сертификатов открытых ключей;

h) порядок синхронизации с всемирным координированным временем (UTC).

Статья 8. Аккредитация поставщика доверительных услуг

(1) Поставщик доверительных услуг получает квалифицированный статус после прохождения процедуры аккредитации.

(2) Квалифицированные поставщики доверительных услуг подлежат аккредитации в соответствии с положениями настоящего Закона.

(3) Аккредитация поставщика доверительных услуг осуществляется органом надзора и контроля на основании поданного заявления. Аккредитация поставщика доверительных услуг является бесплатной и предоставляется сроком на 5 лет, если в заявлении на аккредитацию не указан более короткий срок.

(4) Орган надзора и контроля на основании представленных документов в течение 30 дней принимает решение об аккредитации поставщика доверительных услуг или об отказе в аккредитации.

(5) Поставщик доверительных услуг считается квалифицированным со дня выдачи сертификата аккредитации.

(6) Порядок и подробные требования о том, как подавать заявку, выдавать, приостанавливать и отзывать свидетельство об аккредитации квалифицированного поставщика доверительных услуг, устанавливаются Правительством.

(7) Порядок подачи заявления, предоставления, приостановления и отзыва сертификата аккредитации поставщика квалифицированных доверительных услуг изложен в Законе № 160/2011 о регулировании посредством выдачи разрешения предпринимательской деятельности в части, нерегламентированной настоящим Законом.

(8) Информация об аккредитованных квалифицированных поставщиках доверительных услуг и тех, у кого отозвана аккредитация, публикуется органом надзора и контроля на своей официальной странице в сети Интернет.

(9) Квалифицированные поставщики доверительных услуг обязаны в течение всего периода аккредитации обеспечивать соблюдение требований, в соответствии с которыми они были аккредитованы. Если возникают обстоятельства, которые делают невозможным обеспечение соблюдения этих требований, квалифицированный поставщик доверительных услуг должен уведомить об этом орган надзора и контроля в течение 24 часов.

(10) Неквалифицированные поставщики доверительных услуг обязаны уведомлять орган надзора и контроля не позднее чем за 10 дней о любых изменениях в процедурах обеспечения безопасности и сертификации с указанием даты и времени, когда изменения вступили или вступят в силу.

(11) Квалифицированный поставщик доверительных услуг высшего уровня не подлежит аккредитации в соответствии с положениями настоящего Закона.

Статья 9. Деятельность поставщика доверительных услуг

(1) Поставщик доверительных услуг:

a) создает и выдает сертификаты открытых ключей;

b) приостанавливает и отзывает сертификаты открытых ключей, восстанавливает действие приостановленных сертификатов открытых ключей;

c) ведёт реестр сертификатов открытых ключей, поддерживает его в актуальном состоянии и обеспечивает публичный доступ к реестру;

d) предоставляет на договорной основе доверительные услуги.

(2) Деятельность поставщика доверительных услуг является деятельностью в области криптографической и технической защиты информации и подлежит лицензированию в соответствии с законодательством в области лицензионного регулирования предпринимательской деятельности.

Статья 10. Обязанности поставщика доверительных услуг

(1) Поставщик доверительных услуг обязан:

a) проверять подлинность данных, указанных в заявке на сертификацию открытого ключа, на основании документов, подтверждающих указанные данные;

b) обеспечить соответствие информации в сертификате открытого ключа с информацией, представленной владельцем сертификата открытого ключа;

c) внести сертификат открытого ключа в реестр сертификатов открытых ключей не позднее даты и времени начала срока действия сертификата;

d) обеспечить доступ к реестру сертификатов открытых ключей в соответствии со статьей 52;

e) приостановить действие или отозвать сертификат открытого ключа в случаях, предусмотренных законом, и сделать соответствующую запись в реестре сертификатов открытых ключей в установленные сроки;

f) покрыть ущерб, причиненный любому юридическому или физическому лицу, которое обосновано полагается на данные, содержащиеся в сертификате открытого ключа, выданном поставщиком услуг доверия, в результате того, что он не зарегистрировал отзыв сертификата;

g) уведомить владельца сертификата открытого ключа о фактах, ставших известными поставщику доверительных услуг, которые делают дальнейшее использование закрытого ключа невозможным, и об отзыве сертификата открытого ключа;

h) предоставлять информацию, необходимую для аутентификации доверительных услуг.

(2) Квалифицированный поставщик доверительных услуг обязан, помимо предусмотренных в пункте (1) статьи 10:

1) сертифицировать в установленном законом порядке свой открытый ключ, предназначенный для сертификации открытых ключей;

2) информировать орган надзора и контроля о любом изменении в предоставлении квалифицированных доверительных услуг и о намерении прекратить такую деятельность;

3) использовать безопасные системы для хранения предоставленных ему данных в поддающейся проверке форме, чтобы:

a) они были доступны для исследовательских целей только при условии получения согласия субъекта данных;

b) только уполномоченные лица могли вводить и/или изменять сохраненные данные;

c) подлинность данных могла быть проверена;

4) проверять с помощью соответствующих средств и в соответствии с законом личность и, при необходимости, конкретные признаки физического или юридического лица, которому выдан квалифицированный сертификат. Эта информация должна быть проверена квалифицированным поставщиком доверительных услуг непосредственно или через третью сторону:

a) физическим лицом или уполномоченным представителем юридического лица лично; или

b) дистанционно, с использованием электронных средств идентификации, для которых физическое присутствие физического лица или уполномоченного представителя юридического лица было обеспечено до выдачи квалифицированного сертификата;

c) с помощью сертификата, квалифицированной электронной подписи или квалифицированной электронной печати;

d) с использованием других национально признанных методов идентификации, которые обеспечивают уровень гарантии, эквивалентный по надежности физическому присутствию. Альтернативные методы удаленной идентификации лица определяются Правительством.

5) принимать соответствующие меры против фальсификации и кражи данных;

6) регистрировать в течение определенного периода времени в соответствии со статьей 13 всю соответствующую информацию, относящуюся к квалифицированному сертификату открытого ключа, в частности, для того, чтобы иметь возможность предоставить доказательства сертификации в суде. Записи могут производиться с помощью электронных средств;

7) до вступления в договорные отношения с лицом, запрашивающим сертификат в поддержку доверительной услуги,

информировать это лицо с помощью надежных средств связи о точных условиях использования сертификата, включая ограничения на использование сертификата, существование системы аккредитации и процедуры апелляций и разрешения споров. Информация, передаваемая в электронном виде, должна передаваться в письменном виде на доступном языке. Соответствующие элементы информации также должны предоставляться по запросу третьим лицам, получающим выгоду от сертификата;

8) требовать выдачи дубликата сертификата аккредитации в случае утери или повреждения;

9) регистрировать и сохранять доступной в течение 15 лет, в том числе после прекращения деятельности, всю соответствующую информацию, касающуюся выданных и полученных данных, в частности, для предоставления доказательств в судебных разбирательствах и в целях обеспечения непрерывности обслуживания. Записи могут храниться в электронном виде.

Статья 11. Заявка на сертификацию открытого ключа

(1) Заявка на сертификацию открытого ключа подается в электронной форме, подписанной электронной подписью или электронной печатью, и/или в форме бумажного документа, подписанного рукописной подписью заявителя.

(2) Заявка на сертификацию открытого ключа должна содержать:

a) идентификационные данные заявителя;

b) другие данные заявителя, в зависимости от цели, для которой выдается сертификат открытого ключа, а также информацию, необходимую для связи с заявителем.

Статья 12. Рассмотрение заявки на сертификацию открытого ключа

(1) Заявка на сертификацию открытого ключа рассматривается поставщиком доверительных услуг в течение 5 рабочих дней с даты регистрации запроса, если стороны не договорились об ином.

(2) На основании решения о сертификации открытого ключа Поставщик доверительных услуг создает и выдает сертификат открытого ключа.

(3) Решение об отказе в сертификации открытого ключа принимает поставщик доверительных услуг в случае:

a) подачи заявки на сертификацию открытого ключа в нарушение статьи 11;

b) нарушение прав третьих лиц в процессе подготовки или подачи заявки на сертификацию;

c) предоставление в заявке на сертификацию информации не соответствующей действительности.

(4) Решение об отказе в сертификации открытого ключа может быть оспорено в суде в установленном порядке.

(5) Решение об отказе в сертификации открытого ключа не лишает заявителя права подать новую заявку после устранения всех допущенных нарушений.

Статья 13. Сертификат открытого ключа

(1) При создании сертификата открытого ключа поставщик доверительных услуг обязан проверить уникальность открытого ключа.

(2) Сертификат открытого ключа должен содержать:

a) уникальный регистрационный номер сертификата открытого ключа;

b) идентификационные данные поставщика доверительных услуг, выдавшего сертификат открытого ключа;

c) идентификационные и другие данные владельца сертификата открытого ключа, в зависимости от цели, для которой выдан сертификат, а также информацию, необходимую для связи с владельцем;

d) открытый ключ;

e) дату и время начала периода действия сертификата открытого ключа и дату и время окончания этого периода;

f) данные об используемом криптографическом алгоритме;

g) ограничения на использование сертификата открытого ключа и/или ограничения на стоимость транзакций, в которых он может быть использован, если это применимо;

h) другую информацию, требуемую законом.

(3) Квалифицированный сертификат открытого ключа выдается квалифицированным поставщиком доверительных услуг и должен содержать, кроме того:

a) пометку о том, что сертификат выдан как квалифицированный сертификат открытого ключа;

b) данные проверки электронной подписи или электронной печати, соответствующие данным создания электронной подписи или электронной печати, контролируемым владельцем сертификата открытого ключа, если сертификат выдан для электронных подписей или электронных печатей.

(4) В случае неквалифицированных доверительных услуг структура сертификата открытого ключа определяется поставщиком доверительных услуг в соответствии с положениями настоящего Закона. В случае квалифицированных доверительных услуг структура сертификата открытого ключа определяется органом надзора и контроля в соответствии с положениями настоящего Закона.

(5) На сертификат открытого ключа наносится электронная подпись или электронная печать поставщика доверительных услуг, соответствующая типу запрашиваемого сертификата.

(6) В случаях, установленных законом или по соглашению сторон, поставщик доверительных услуг создает сертификат открытого ключа также в виде бумажного документа в двух экземплярах. Сертификат открытого ключа в форме бумажного документа должен быть подписан рукописными подписями владельца сертификата открытого ключа и уполномоченного лица поставщика услуг доверия. Одна копия сертификата открытого ключа передается владельцу, а другая хранится у поставщика доверительных услуг.

(7) Поставщик доверительных услуг, в согласовании с владельцем сертификата открытого ключа, может указать в сертификате открытого ключа случаи, в которых этот сертификат может быть использован, а также ограничения на его использование.

(8) По просьбе владельца сертификата открытого ключа поставщик доверительных услуг может также указать в сертификате открытого ключа другую информацию, чем указанная в пункте (2) и (3), при условии, что они не противоречат законодательству и не угрожают национальной безопасности или общественному порядку, и только после предварительной проверки точности такой информации.

(9) Поставщик доверительных услуг должен внести сертификат в реестр сертификатов открытых ключей не позднее даты и времени начала срока действия сертификата.

Статья 14. Закрытый ключ и открытый ключ

(1) Закрытый ключ и открытый ключ, используемые для создания доверительных услуг, создаются физическим или юридическим лицом. Они могут быть созданы третьими лицами с явного согласия заинтересованного лица при условии, что будет обеспечена невозможность копирования этих ключей.

(2) Закрытый ключ и связанный с ним открытый ключ создаются одновременно.

(3) Физическое или юридическое лицо может владеть неограниченным количеством закрытых и открытых ключей.

(4) Закрытый ключ используется исключительно его владельцем таким образом, чтобы исключить доступ к нему другого лица.

Открытый ключ сертифицируется поставщиком доверительных услуг и доступен каждому.

Статья 15. Срок действия и хранения сертификата открытого ключа

(1) Срок действия сертификата открытого ключа поставщика доверительных услуг высшего уровня составляет 20 лет, срок действия сертификата открытого ключа поставщика доверительных услуг второго уровня составляет 10 лет, срок действия сертификата открытого ключа пользователя определяется поставщиком доверительных услуг, но не

может быть более 5 лет, в зависимости от возможностей технических средств создания электронной подписи.

(2) Поставщик доверительных услуг обязан хранить сертификат открытого ключа не менее 15 лет с даты отзыва или истечения срока действия сертификата.

Статья 16. Приостановление и отзыв сертификата открытого ключа

(1) Поставщик доверительных услуг приостанавливает действие сертификата открытого ключа по требованию владельца сертификата открытого ключа.

(2) Поставщик доверительных услуг отзывает сертификат открытого ключа:

a) по требованию владельца сертификата открытого ключа;

b) по требованию руководителя юридического лица, в котором действует владелец сертификата открытого ключа, в случае сертификатов, выданных владельцам для представительства юридического лица;

c) при обнаружении неправдивой информации в заявке на сертификацию открытого ключа или в сертификате открытого ключа;

d) нарушение конфиденциальности закрытого ключа (компрометация закрытого ключа);

e) по истечении срока, на который было приостановлено действие сертификата открытого ключа, в отсутствие заявки со стороны владельца сертификата открытого ключа на восстановление его действия;

f) при внесении изменений в сертификат открытого ключа;

g) в случае смерти владельца сертификата открытого ключа или в случае установления в отношении него мер юридической опеки (временная опека, опекунство или попечительство);

h) по требованию надзорного и контрольного органа, в случае нарушения настоящего закона;

(3) При получении информации о необходимости отзыва сертификата открытого ключа поставщик доверительных услуг обязан в течение трех рабочих часов внести соответствующие записи в регистр сертификатов открытых ключей .

(4) Поставщик услуг доверия обязан уведомить владельца сертификата открытого ключа о причинах отзыва его сертификата, если процедура отзыва не была инициирована самим владельцем.

Статья 17. Обязанности владельца сертификата открытого ключа

Владелец сертификата открытого ключа обязан:

1) обеспечить необходимые условия для исключения доступа другого лица к его закрытому ключу;

2) не использовать закрытый ключ для доверительных услуг, если у него есть основания полагать, что нарушена конфиденциальность закрытого ключа;

3) незамедлительно потребовать приостановления действия сертификата открытого ключа или его отзыва, если:

a) утерян свой закрытый ключ;

b) есть основания полагать, что конфиденциальность закрытого ключа была нарушена;

c) информация, содержащаяся в сертификате открытого ключа, не соответствует действительности;

4) уведомлять в течение 24 часов поставщика доверительных услуг о любых изменениях информации, содержащейся в сертификате открытого ключа;

5) выполнять другие обязанности, предусмотренные настоящим Законом и договором, заключенным с поставщиком доверительных услуг.

Статья 18. Регистр сертификатов открытых ключей

(1) Поставщик доверительных услуг обязан вести регистр сертификатов открытых ключей.

(2) Регистр сертификатов открытых ключей должен содержать:

a) действительные сертификаты открытых ключей;

b) отозванные и приостановленные сертификаты открытых ключей;

c) дату и время выдачи сертификатов открытых ключей;

d) дату и время отзыва сертификатов открытых ключей;

e) иную информацию в соответствии с нормативными документами в области доверительных услуг.

(3) Для проверки подлинности доверительных услуг поставщик доверительных услуг обязан предоставить свободный доступ к регистру сертификатов открытых ключей, в том числе в режиме реального времени.

Раздел 2
Электронная подпись и электронная печать

Статья 19. Принципы использования электронной подписи и электронной печати

Принципами использования электронной подписи и электронной печати являются:

a) свобода выбора и использования любого вида электронной подписи или электронной печати, если нормативными актами или соглашением сторон не предусмотрено требование об использовании конкретного вида электронной подписи или электронной печати в соответствии с целями их использования;

b) возможность выбора любых технологий и/или технических средств, позволяющих использовать конкретные виды электронных подписей или электронных печатей в соответствии с положениями настоящего закона;

c) невозможность ссылаться на отсутствие юридической силы электронной подписи или электронной печати и/или электронного документа, на котором она проставлена, только на том основании, что электронная подпись или электронная печать была создана с помощью определенного устройства и/или продукта для создания электронной подписи или электронной печати.

Статья 20. Виды электронных подписей и электронных печатей

Видами электронных подписей и электронных печатей, принципы и механизмы использования которых регулируются настоящим Законом, являются:

a) усиленная;

b) квалифицированная.

Статья 21. Правовой режим использования электронных подписей и электронных печатей

(1) Электронные подписи и электронные печати, независимо от степени их защиты, имеют юридические последствия и допустимы в качестве доказательств, в том числе в судебном процессе, даже если:

a) имеют электронную форму; или

b) не основаны на сертификате, выданным поставщиком доверительных услуг; или

c) не основаны на квалифицированном сертификате открытого ключа; или

d) не созданы с использованием устройства создания электронной подписи или электронной печати.

(2) Квалифицированная электронная подпись имеет такое же юридическое значение, как и собственноручная подпись.

(3) Квалифицированные электронные подписи и квалифицированные электронные печати пользуются презумпцией целостности данных и правильности происхождения данных, к которым относится электронная подпись или квалифицированная электронная печать.

(4) Порядок обеспечения необходимой степени защиты квалифицированной электронной подписи для приравнивания ее к рукописной подписи на бумаге определяется органом надзора и контроля в соответствии с полномочиями, предусмотренными частью (2) статьи 35.

(5) Порядок применения электронной подписи должностными лицами юридическими лицами публичного права определяется Правительством. Юридические лица частного права самостоятельно

определяют порядок применения электронных подписей своими представителями.

Статья 22. Ограничения на использование некоторых видов электронных подписей или электронных печатей

(1) Использование усиленной электронной подписи и усиленной электронной печати не допускается:

a) на электронных документах, содержащих сведения, отнесенные к государственной тайне;

b) на электронных документах в правоотношениях юридических лиц публичного права с физическими и юридическими лицами частного права.

(2) В отступление от положений пункта (1), подпункт a), допускается подписание электронных документов, содержащих сведения, отнесенные к государственной тайне, усиленной электронной подписью лицами, идентичность и статус которых в соответствии с положениями Закона № 245/2008 о государственной тайне составляют государственную тайну, из состава Службы информации и безопасности, Национального центра по борьбе с коррупцией и Министерства внутренних дел в рамках электронного оборота их документов.

Статья 23. Требования к усиленным электронным подписям и электронным печатям

Усиленные электронные подписи или электронные печати должны в совокупности отвечать следующим требованиям:

a) относятся исключительно к владельцу;

b) позволяют идентифицировать владельца;

c) создаются с использованием данных для создания электронной подписи или электронных печатей, которые подписант или создатель печати может использовать с высокой степенью уверенности, исключительно под своим контролем;

d) связаны с данными, к которым они относятся так, что любые последующие изменения этих данных могут быть обнаружены.

Статья 24. Требования к квалифицированным электронным подписям и электронным печатям

Квалифицированные электронные подписи или электронные печати отвечают всем требованиям усиленных электронных подписей или электронных печатей, а также дополнительно:

a) основаны на квалифицированном сертификате открытого ключа, выданном квалифицированным поставщиком доверительных услуг;

b) создаются с помощью устройства создания электронной подписи или электронной печати и проверяются с помощью устройства проверки

электронной подписи или электронной печати и/или продукта, которые имеют подтверждение соответствия требованиям настоящего Закона.

Статья 25. Требования к квалифицированным сертификатам для электронных подписей или электронных печатей

Квалифицированные сертификаты для электронных подписей или электронных печатей содержат:

a) пометку в машинообрабатываемой форме, что сертификат был выдан в качестве квалифицированного сертификата для электронных подписей или электронных печатей;

b) идентификационные данные квалифицированного поставщика доверительных услуг, выдающего квалифицированные сертификаты;

c) идентификационные и другие данные лица, подписавшего или создавшего электронную печать;

d) данные проверки электронных подписей или электронных печатей, соответствующие данным об их создании;

e) дату и время начала периода действия сертификата и дату и время окончания этого периода;

f) уникальный регистрационный номер сертификата;

g) данные проверки квалифицированного сертификата электронной подписи или электронной печати, соответствующие данным их создания;

h) квалифицированную электронную подпись или электронную печать эмитента квалифицированного поставщика доверительных услуг, или;

i) усиленную электронную подпись или электронную печать выдающего квалифицированного поставщика доверительных услуг, домицилированного или учрежденного в другом государстве, в случае квалифицированных сертификатов электронных подписей или электронных печатей, признанных в соответствии со статьей 3, или;

j) усиленную электронную подпись или усиленную электронную печать поставщика доверительных услуг более высокого уровня в случае квалифицированных сертификатов электронных подписей или электронных печатей аккредитованных поставщиков доверительных услуг.

Статья 26. Создание электронной подписи или электронной печати

(1) Создание электронной подписи или электронной печати осуществляется с помощью устройства создания электронной подписи или электронной печати и/или продукта с использованием данных для создания электронной подписи или электронной печати.

(2) Генерация или управление данными для создания квалифицированной электронной подписи или квалифицированной электронной печати от имени лица, подписавшего или создавшего печать,

может осуществляться квалифицированным поставщиком доверительных услуг только с согласия владельца сертификата открытого ключа.

Статья 27. Требования к устройствам для создания электронных подписей или электронных печатей

(1) Устройства для создания усиленных или квалифицированных электронных подписей или электронных печатей должны обеспечивать с помощью соответствующих технических средств и процедур, по крайней мере, следующее:

a) данные о создании электронной подписи или электронной печати могут появиться только один раз и их конфиденциальность обеспечивается в соответствии с настоящим законом;

b) данные о создании электронной подписи или электронной печати не могут быть вычислены расчетным путем, а электронная подпись или электронная печать защищены от возможной подделки доступными на тот момент техническими средствами;

c) данные для создания электронной подписи или электронной печати надежно защищены законным лицом, подписавшим или создавшим их, от использования другими лицами;

d) предоставляют возможность отображения содержания электронного документа, к которому применена электронная подпись или электронная печать, или однозначно ссылаются на данный документ;

e) электронная подпись или электронная печать создается только после того, как подписант или создатель печати подтвердил создание электронной подписи или электронной печати;

f) однозначно подтверждают создание электронной подписи или электронной печати.

(2) Генерирование или управление данными для создания электронной подписи или электронной печати от имени лица, подписавшего или создавшего печать, может осуществляться только квалифицированным поставщиком доверительных услуг.

(3) Усиленные или квалифицированные устройства для создания электронной подписи или электронной печати не должны изменять данные, к которым применяется усиленная или квалифицированная электронная подпись или электронная печать, или препятствовать их представлению подписавшему или создавшему их лицу до подписания или скрепления печатью.

Статья 28. Проверка подлинности электронной подписи или электронной печати

(1) Проверка подлинности электронной подписи или электронной печати осуществляется с помощью устройства проверки электронной

подписи или электронной печати и/или продукта с использованием данных для проверки электронной подписи или электронной печати.

(2) При проверке усиленной электронной подписи или усиленной электронной печати и квалифицированной электронной подписи или квалифицированной электронной печати устройство и/или изделие для проверки электронной подписи или электронной печати должно:

a) предлагать возможность отображения содержания электронного документа или однозначно ссылатся на данный документ;

b) отображать факт изменения электронного документа;

c) относятся к подписавшему или создавшему электронную печать.

(3) При проверке усиленной электронной подписи или электронной печати, а также квалифицированной электронной подписи и электронной печати должно быть с достаточной степенью уверенности установлено, что:

a) данные проверки электронной подписи или электронной печати соответствуют данным, отображаемым лицу, проверяющему электронную подпись или электронную печать;

b) электронная подпись или электронная печать проверяется с уверенностью и результат проверки и личность подписавшего или создателя печати отображаются правильно;

c) подлинность и действительность сертификата открытого ключа, запрашиваемого в момент проверки электронной подписи или электронной печати, проверены с уверенностью;

d) четко воспроизводится содержание сертификата открытого ключа;

e) могут быть обнаружены любые изменения, которые могут повлиять на безопасность электронной подписи или электронной печати.

Статья 29. Требования к проверке квалифицированной электронной подписи и печати

Процесс проверки квалифицированной электронной подписи или электронной печати подтверждает ее действительность при соблюдении следующих условий:

a) сертификат, лежащий в основе электронной подписи или электронной печати, на момент подписания или запечатывания являлся квалифицированным сертификатом электронной подписи или электронной печати в соответствии со статьей 25;

b) квалифицированный сертификат был выдан квалифицированным поставщиком доверительных услуг и был действителен на момент применения электронной подписи или электронной печати;

c) данные проверки электронных подписей или электронных печатей соответствуют данным, предоставленным держателем сертификата открытого ключа;

d) уникальный набор данных, представляющий подписанта или создателя электронной печати в сертификате, правильно предоставлен владельцу сертификата с открытым ключом;

e) использование псевдонима четко указано владельцу сертификата открытого ключа, если псевдоним был использован во время подписания;

f) электронная подпись или электронная печать была создана квалифицированным устройством для создания электронной подписи или электронной печати;

g) целостность данных, к которым была применена электронная подпись или электронная печать, не была нарушена;

h) требования, изложенные в статье 23, были выполнены на момент подписания.

Раздел 3
Электронные метки времени

Статья 30. Юридическая сила электронных меток времени

(1) Электронной метке времени не может быть отказано в юридической силе и допустимости в качестве доказательства в судебном процессе только на основании того, что она находится в электронной форме или она не отвечает требованиям, предъявляемым к квалифицированной электронной метке времени.

(2) Квалифицированная электронная метка времени считается точной в отношении даты и времени, на которые она указывает, а также в отношении целостности данных, к которым относятся указанные дата и время.

Статья 31. Требования к электронным меткам времени

(1) Требования к усиленным электронным меткам времени устанавливаются поставщиками доверительных услуг.

(2) Квалифицированная электронная метка времени выдается квалифицированным поставщиком доверительных услуг и отвечает следующим требованиям:

a) обеспечивает связь между датой и временем и данными таким образом, чтобы разумно исключить возможность изменения данных без обнаружения;

b) основана на источнике точного времени, привязанном к всемирному координированному времени;

c) на ней нанесена квалифицированная электронная подпись или квалифицированная электронная печать квалифицированного поставщика доверительных услуг или усиленная электронная подпись или усиленная электронная печать выдающего квалифицированного поставщика доверительных услуг, домицилированного или учрежденного в другом

государстве, в случае штампов времени, признаваемых в соответствии со статьей 3.

Раздел 4
Служба зарегистрированной электронной рассылки и аутентификации веб-страниц

Статья 32. Юридическая сила службы зарегистрированной электронной доставки

(1) Данным, переданным и полученным с использованием службы зарегистрированной электронной доставки, не может быть отказано в юридической силе и допустимости в качестве доказательства в судебном процессе только на том основании, что они находятся в электронной форме или что они не соответствуют требованиям, предъявляемым к квалифицированной службе зарегистрированной электронной доставки.

(2) Данные, отправленные и полученные с помощью квалифицированной службы зарегистрированной электронной доставки, являются полными, отправлены идентифицированным отправителем и получены идентифицированным получателем, а также отправлены и получены службой зарегистрированной электронной доставки в точное время.

Статья 33. Требования к квалифицированным службам зарегистрированной электронной доставки

Квалифицированные службы зарегистрированной электронной доставки отвечают следующим требованиям:

a) предоставляются одним или несколькими квалифицированными поставщиками доверительных услуг;

b) обеспечивает идентификацию отправителя;

c) обеспечивает идентификацию получателя до предоставления данных;

d) отправка и получение данных защищены электронной подписью или электронной печатью квалифицированного поставщика доверительных услуг, чтобы исключить возможность обмена данными без обнаружения;

e) любое изменение данных, необходимое для целей отправки или получения данных, четко указывается отправителю и получателю данных;

f) дата и время отправки, получения и любого изменения данных указывается квалифицированным электронной меткой времени.

Статья 34. Требования к квалифицированным сертификатам для аутентификации веб-страниц

Квалифицированные сертификаты для аутентификации веб-страниц должны содержать:

a) пометку в машинообрабатываемой форме, что сертификат был выдан в качестве квалифицированного сертификата для аутентификации веб-страницы;

b) идентификационные данные квалифицированного поставщика доверительных услуг, выдающего квалифицированные сертификаты;

c) идентификационные и другие данные владельца сертификата открытого ключа, а также информация, необходимая для связи с владельцем;

d) дату и время начала периода действия сертификата и дату и время окончания этого периода;

e) имя домена (доменов), управляемого владельцем сертификата открытого ключа, которому был выдан сертификат;

f) уникальный регистрационный номер сертификата;

g) квалифицированную электронную подпись или электронную печать квалифицированного поставщика доверительных услуг или усиленную электронную подпись или электронную печать квалифицированного поставщика доверительных услуг, домицилированного или учрежденного в другом государстве, в случае квалифицированных сертификатов для аутентификации веб-сайта, признанного в соответствии со статьей 3;

h) данные проверки квалифицированного сертификата для аутентификации веб-страницы, соответствующие данным о ее создании.

Глава III
НАДЗОР И КОНТРОЛЬ

Статья 35. Орган надзора и контроля

(1) Органом надзора и контроля является Служба информации и безопасности Республики Молдова.

(2) Орган надзора и контроля выполняет следующие задачи:

a) отвечает за разработку и продвижение государственной политики и осуществление контроля в области доверительных услуг;

b) проводит аккредитацию поставщиков доверительных услуг и отзывает соответствующий статус;

c) выполняет функции квалифицированного поставщика доверительных услуг высшего уровня для квалифицированных поставщиков доверительных услуг;

d) обеспечивает ведение, обновление и публичный доступ к данным Регистра поставщиков доверительных услуг;

e) ведет и публикует, в защищенном виде, защищенные списки с электронной подписью или электронной печатью органа надзора и контроля, которые включают информацию о квалифицированных поставщиках доверительных услуг и информацию о предоставляемых ими

квалифицированных доверительных услугах, в машинообрабатываемой форме;

f) разрабатывает и утверждает посредством нормативных актов требования в области доверительных услуг;

g) осуществляет мониторинг и контроль соблюдения требований при оказании доверительных услуг;

h) участвует в разработке и утверждении технических регламентов и стандартов в области доверительных услуг;

i) оказывает по запросу методическую и практическую помощь в использовании доверительных услуг;

j) осуществляет надзор за квалифицированными поставщиками доверительных услуг в отношении качества и безопасности предоставляемых ими квалифицированных доверительных услуг, а также за выполнением требований, установленных настоящим Законом;

k) приостанавливает или отзывает аккредитацию поставщика доверительных услуг, если он не соответствует требованиям в области доверительных услуг;

l) сотрудничает с национальным органом по защите персональных данных, в частности, информируя его без неоправданной задержки о результатах проверок квалифицированных поставщиков доверительных услуг, в отношении которых предположительно были нарушены правила защиты персональных данных;

m) требует от поставщиков доверительных услуг устранить любое несоблюдение требований настоящего Закона;

n) осуществляет международное сотрудничество в области доверительных услуг.

(3) Орган или государственное учреждение, ответственное за предоставление услуги синхронизации с всемирным координированным временем (UTC) из одного источника, устанавливается Правительством.

Статья 36. Контроль в области доверительных услуг

(1) Контроль за соблюдением требований, установленных настоящим Законом, при предоставлении доверительных услуг, выдаче или продлении аккредитации осуществляется органом надзора и контроля.

(2) Контроль осуществляется Комиссией по контролю за доверительными услугами (*далее - Комиссия*) на основании положения, утвержденного органом надзорна и контроля.

(3) Комиссия создается в составе органа надзорна и контроля на основании приказа о контроле, изданного руководителем этого органа.

(4) Номинальный состав Комиссии определяется в каждом конкретном случае.

(5) Комиссия имеет право:

a) иметь свободный доступ к документальным материалам в бумажном и электронном формате, необходимым для выполнения работ, связанных с оказанием доверительных услуг, а также к системам распространения программного обеспечения, программным приложениям и установленному оборудованию;

b) получить полную информацию об условиях и способах использования оборудования и программного обеспечения;

c) получить от ответственных лиц и сотрудников поставщика доверительных услуг информацию о предоставлении доверительных услуг, подлежащих контролю;

d) иметь доступ в помещения поставщика доверительных услуг в течение рабочего дня (в период проведения проверки).

(6) Комиссия не имеет права проводить проверку без предъявления распоряжения о проведении проверки и документов, удостоверяющих личность членов комиссии.

(7) При осуществлении контроля за соблюдением условий, установленных настоящим Законом, Комиссия принимает во внимание следующие правила:

a) законность и соблюдение компетенции, установленной законом;

b) не допускает применения санкций, не установленных законом;

c) трактовать сомнения, возникающие при применении законодательства, в пользу поставщика доверительных услуг;

d) осуществление контроля за государственный счет;

e) предписание рекомендаций по устранению нарушений, выявленных в ходе проверки;

f) право поставщика доверительных услуг оспаривать действия органа надзора и контроля, в том числе в судебном порядке.

(8) Плановые проверки соблюдения квалифицированным поставщиком доверительных услуг обязательств, предусмотренных настоящим Законом, проводятся органом надзора и контроля не чаще одного раза в течение календарного года с привлечением, при необходимости, представителей учреждений с регулирующими и контрольными функциями, в соответствии с компетенциями.

(9) Планы проверок, составленные органом надзора и контроля и утвержденные в установленном порядке, должны быть согласованы с руководством поставщика доверительных услуг не менее чем за 5 рабочих дней до начала проверок в установленные сроки.

(10) Внеплановые проверки проводятся по решению органа надзора и контроля только на основании:

a) выявление и подтверждение органом надзора и контроля нарушений настоящего Закона; и/или

b) получение мотивированных запросов и жалоб в письменной форме в орган надзора и контроля по поводу нарушений или

ненадлежащего исполнения поставщиком доверительных услуг обязанностей, предусмотренных настоящим Законом.

(11) Поставщик доверительных услуг информируется о внеплановой проверке в день ее начала.

(12) Повторные проверки проводятся только с целью проверки исполнения предписания об устранении нарушений настоящего Закона, указанного в акте предыдущего контроля (планового или внепланового). Повторная проверка считается частью предыдущей проверки.

(13) Контроль должен осуществляться строго в сроки, указанные в распоряжении о проведении контроля.

(14) Срок проведения плановой проверки и внеплановой проверки не может превышать 10 рабочих дней, а повторной проверки - 5 рабочих дней. В случае внеплановых проверок 10-дневный срок может быть продлен еще на 10 дней руководителем органа надзора и контроля на основании мотивированного решения, доведенного до сведения проверяемого поставщика доверительных услуг, которое может быть оспорено поставщиком доверительных услуг.

(15) При осуществлении контроля за соблюдением обязательств, предусмотренных настоящим Законом, лицо, оказывающее доверительные услуги, представляет информацию и документы, относящиеся к цели контроля, и не препятствует проведению контроля.

(16) По результатам проверки составляется акт в двух экземплярах, один из которых направляется/доставляется поставщику доверительных услуг не позднее 5 рабочих дней после окончания проверки, а второй хранится в органе надзора и контроля. Если поставщик доверительных услуг не согласен с результатами проверки, он может в течение 10 рабочих дней с момента получения акта проверки представить письменное объяснение своего несогласия и приложить соответствующие документы.

(17) В случае выявления нарушений обязательств, предусмотренных настоящим Законом, орган надзора и контроля на основании акта контроля выдает предписание об устранении таких нарушений, включая рекомендации по устранению всех выявленных нарушений, а также предупреждение о возможном приостановлении или отзыве аккредитации, если они не будут устранены в установленный срок.

(18) Срок устранения выявленных нарушений составляет 15 рабочих дней, исчисляемых со дня, следующего за днем получения предписания, направленного/врученного вместе с актом проверки.

(19) Если поставщик доверительных услуг не устранил все выявленные нарушения в установленный срок, по официальному запросу поставщика доверительных услуг срок устранения нарушений продлевается на срок, запрошенный поставщиком доверительных услуг, но не более чем на 20 рабочих дней.

(20) Квалифицированный поставщик доверительных услуг, получивший предписание об устранении нарушений обязательств, предусмотренных настоящим Законом, обязан в течение срока, указанного в предписании, сообщить информацию об устранении нарушений органу надзора и контроля.

(21) Информация о результатах проверки публикуется органом надзора и контроля на своей официальном веб-странице.

(22) Поставщик доверительных услуг имеет право подавать письменные жалобы в орган надзора и контроля на нарушения положений настоящего Закона, допущенные Комиссией, или оспаривать ее действия в суде.

Статья 37. Приостановление и восстановление аккредитации

(1) Аккредитация приостанавливается в соответствии с законодательством в области регулирования предпринимательской деятельности.

(2) Основаниями для принятия предусмотренных законом мер по приостановлению аккредитации являются следующие:

a) запрос квалифицированного поставщика доверительных услуг о приостановлении аккредитации;

b) нарушение поставщиком доверительных услуг обязательств, предусмотренных настоящим Законом;

c) выявление недостоверных данных в документах, представленных в орган надзора и контроля;

d) недействительность банковской гарантии или страхового полиса;

e) невыполнение поставщиком доверительных услуг предписания об устранении нарушений, предусмотренных настоящим Законом, выявленных в результате контроля Комиссии.

(3) Решение о приостановлении аккредитации доводится до сведения квалифицированного поставщика доверительных услуг в течение 3 рабочих дней со дня его принятия. Срок приостановления аккредитации не может превышать 2 месяца.

(4) Поставщик квалифицированных доверительных услуг обязан письменно уведомить орган надзора и контроля об устранении обстоятельств, приведших к приостановлению аккредитации.

(5) Решение о восстановлении действия аккредитации принимается органом надзора и контроля на основании решения суда, вынесшего решение о приостановлении действия аккредитации, или вышестоящего суда в течение 3 рабочих дней со дня получения уведомления. Решение должно быть доведено до сведения поставщика доверительных услуг в течение 3 рабочих дней с даты его принятия.

(6) Срок действия аккредитации не продлевается в период приостановления аккредитации.

Статья 38. Отзыв аккредитации

(1) Аккредитация отзывается в соответствии с законодательством в области регулирования предпринимательской деятельности.

(2) Основанием для совершения предусмотренных законом действий по отзыву аккредитации являются следующие:

a) заявление квалифицированного поставщика доверительных услуг о прекращении деятельности, поданное за 30 дней до планируемого прекращения деятельности;

b) решение об аннулировании государственной регистрации индивидуального предпринимателя или юридического лица, в рамках которого осуществляет свою деятельность поставщик доверительных услуг;

c) факт передачи аттестата аккредитации или его копии другому лицу для осуществления аккредитованного вида деятельности;

d) не устранение в установленный срок обстоятельств, приведших к приостановлению аккредитации;

e) неоднократное невыполнение требований по устранению нарушений обязательств, установленных настоящим Законом.

(3) Дата и номер решения об отзыве аккредитации вносятся в Реестр поставщиков доверительных услуг не позднее рабочего дня, следующего за днем принятия решения.

(4) Все сертификаты открытых ключей, выданные прекратившим свою деятельность квалифицированным поставщиком доверительных услуг, должны быть аннулированы и переданы на хранение другому квалифицированному поставщику доверительных услуг в порядке, определенном органом надзора и контроля, за счет прекратившего свою деятельность поставщика доверительных услуг.

(5) Квалифицированный поставщик доверительных услуг обязан в течение 10 рабочих дней со дня принятия решения об отзыве аккредитации представить в орган надзора и контроля отозванный аттестат аккредитации.

Статья 39. Требования безопасности для поставщиков доверительных услуг

(1) Квалифицированные и неквалифицированные поставщики доверительных услуг должны применять соответствующие технические и организационные меры для управления рисками безопасности доверительных услуг, которые они предоставляют.

(2) Квалифицированные и неквалифицированные поставщики доверительных услуг должны немедленно, но не позднее 24 часов с момента обнаружения, уведомить орган надзора и контроля о любом нарушении безопасности или потере целостности, которое оказывает существенное влияние на предоставляемую доверительную услугу или

хранящиеся в ней персональные данные. Если нарушение безопасности или потеря целостности может негативно повлиять на физическое или юридическое лицо, которому была предоставлена услуга доверия, поставщик услуг доверия также должен уведомить соответствующее физическое или юридическое лицо о нарушении безопасности или потере целостности без неоправданной задержки.

(3) Уведомленный орган надзора и контроля информирует общественность или просит поставщика доверительных услуг сделать это, если он считает, что раскрытие информации о нарушении безопасности или потере целостности отвечает общественным интересам.

Глава IV
ПРАВОВОЙ РЕЖИМ ЭЛЕКТРОННОГО ДОКУМЕНТА И ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Статья 40. Правовой режим использования электронного документа

(1) Электронный документ, подписанный квалифицированной электронной подписью, по своим последствиям приравнивается к аналогичному бумажному документу, подписанному рукописной подписью.

(2) Электронный документ, подписанный другим типом электронной подписи кроме квалифицированной, приравнивается по своим последствиям к аналогичному документу на бумажном носителе, подписанному рукописной подписью, только в случаях, прямо предусмотренных нормативными актами или соглашением сторон о применении электронных подписей или печатей, при соблюдении условий, установленных в части (1) статьи 43.

(3) Нормативные акты или соглашение сторон о применении электронных подписей, определяющие случаи признания электронных документов, подписанных с другим типом электронной подписи чем квалифицированный, приравненные по своим последствиям к аналогичным документам на бумаге, подписанным рукописной подписью, должны предусматривать порядок проверки электронной подписи, а также обязательства сторон в отношении конфиденциальности и материальной ответственности.

(4) Если закон требует, чтобы документ был заполнен или представлен в бумажной форме и подписан собственноручной подписью, считается, что электронный документ соответствует этому требованию.

(5) Если законодательство требует, чтобы бумажный документ был заверен печатью, считается, что электронный документ соответствует этому требованию.

(6) Одна электронная подпись или электронная печать может быть применена к нескольким связанным документам (набору электронных

документов).

(7) Использование электронных документов в судебных разбирательствах регулируется процессуальным законодательством.

(8) Электронный документ по своей доказательной силе приравнивается к письменным доказательствам или физическим средствам доказывания и не может быть отвергнут в качестве доказательства только потому, что он находится в электронной форме.

(9) Если законодательством предусмотрена государственная регистрация документа, то электронный документ подлежит регистрации.

(10) Все идентичные копии электронного документа считаются оригиналами и имеют одинаковую юридическую силу.

(11) Если лицо создает электронный документ и бумажный документ подписанный рукописной подписью, идентичный по содержанию, оба рассматриваются как самодостаточные и оригинальные документы.

(12) Копией электронного документа считается его представление (визуализация) на бумаге в воспринимаемой форме. Копия электронного документа должна быть заверена в порядке, установленном законом для заверения копий бумажных документов, и должна содержать пометку о том, что она является копией электронного документа.

Статья 41. Области и цели использования электронного документа

(1) Электронный документ может быть использован физическими и юридическими лицами во всех сферах деятельности, в которых возможно использование аппаратных и программных средств, позволяющих создавать, обрабатывать, отправлять, получать, хранить, изменять и/или уничтожать информацию в электронной форме.

(2) Электронный документ может использоваться для передачи информации, ведения переписки, составления юридических документов и как документ, отражающий экономические факты.

Статья 42. Требования к электронным документам

Электронный документ должен отвечать следующим основным требованиям:

a) быть созданным, обработанным, отправленным, полученным, сохраненным, измененным и/или уничтоженным с помощью аппаратного и/или программного обеспечения;

b) содержать для подтверждения своей подлинности одну или несколько электронных подписей или печатей, отвечающих условиям и требованиям, установленным настоящим Законом;

c) создаваться и использоваться методами и в форме, позволяющей идентифицировать подписанта или создателя электронной печати;

d) быть отображенным в различимой форме;

e) для многократного использования.

Статья 43. Подлинность электронного документа

(1) Электронный документ считается подлинным, если он соответствует следующим условиям:

a) электронная подпись или электронная печать применяется лицом, уполномоченным в установленном порядке подписывать рукописной подписью эквивалентный бумажный документ;

b) на документе проставлена электронная подпись или подлинная электронная печать подписавшего лица или создателя печати, указанного в документе.

(2) Проверка подлинности электронного документа осуществляется путем проверки подлинности электронной подписи или электронной печати и/или изделия с помощью устройств проверки электронной подписи или электронной печати.

Статья 44. Организация электронного документооборота

(1) Электронный документооборот организуется в соответствии с положениями настоящего Закона и правилами, установленными владельцем системы электронного документооборота, а также в соответствии с договорами, заключенными между субъектами электронного документооборота.

(2) Электронный документооборот может включать:

a) создание и обработка электронного документа с применением электронной подписи или электронной печати;

b) отправка и получение электронного документа;

c) проверка подлинности электронного документа;

d) подтверждение получения электронного документа;

e) электронный учет документов;

f) хранение, изменение и/или уничтожение электронного документа;

g) создание дополнительных копий электронного документа;

h) создание и заверение копий электронного бумажного документа;

i) применение метки времени.

(3) Порядок создания, обработки, отправки, получения, хранения, изменения и/или уничтожения электронного документа для систем электронного документооборота юридических лиц, регулируемых публичным правом, определяются Правительством, а для систем электронного документооборота юридических лиц, регулируемых частным правом, - их владельцами.

Статья 45. Посредник в электронном документообороте

(1) Посредники могут участвовать в организации и осуществлении электронного документооборота на условиях настоящего закона и в

соответствии с правилами, установленными владельцем системы электронного документооборота.

(2) Посредник в электронном документообороте обязан:

a) иметь аппаратные и/или программные средства, обеспечивающие надежность и безопасность используемых информационных систем;

b) иметь персонал, обладающий компетенцией и опытом в области информационных технологий и/или информационной безопасности;

c) обеспечить необходимые условия для определения точного времени и источника отправки электронного документа, а также времени получения и электронного адреса получателя;

d) обеспечить защиту и сохранность электронных документов;

e) хранить электронные документы в соответствии с договором с пользователями системы электронного документооборота.

Статья 46. Создание электронного документа

(1) Электронный документ содержит информацию, составляющую содержание электронного документа, и электронную подпись или электронную печать подписавшего лица или создателя электронной печати.

(2) Создание электронного документа завершается нанесением электронной подписи или электронной печати подписавшим или создателем электронной печати и, если это применимо, проставлением штампа времени.

Статья 47. Отправка и получение электронного документа

(1) Электронный документ может быть отправлен и получен с использованием электронных информационно-коммуникационных систем и/или физических носителей.

(2) Электронный документ отправляется в форме, позволяющей получателю хранить и использовать его.

(3) Если между подписавшим или создателем печати и адресатом электронного документа не согласовано иное, электронный документ считается отправленным, если:

a) отправляется лицом, подписавшим или создавшим печать, или посредником в электронном документообороте, действующим от имени лица, подписавшего или создавшего печать, или через информационную систему, используемую лицом, подписавшим или создавшим печать;

b) правильно адресована или направлена в информационную систему, указанную получателем;

c) предоставляется в форме, позволяющей обрабатывать его в информационной системе, указанной получателем;

d) входит в информационную систему, которая не контролируется лицом, подписавшим или создавшим печать, или посредником электронного документа, который отправляет электронный документ от

имени лица, подписавшего или создавшего печать.

(4) Если между лицом, подписавшим электронный документ, и адресатом электронного документа не согласовано иное, электронный документ считается полученным адресатом, если адресат:

a) входит в информационную систему, из которой получатель может получить электронные документы;

b) поступает в указанную получателем информационную систему в форме, доступной для использования в этой системе.

(5) Электронный документ считается неотправленным, если адресат знал или должен был знать, что:

a) лицо, указанное в документе в качестве подписанта, не является истинным подписантом;

b) подписывающее лицо не является инициатором отправки электронного документа ;

c) электронный документ получен получателем с изменениями или без электронной подписи.

(6) Электронный документ не считается полученным, если лицо, получившее его, не является его предполагаемым получателем.

Статья 48. Время отправки и получения электронного документа

(1) Если между лицом, подписавшим или создавшим печать, и адресатом электронного документа не согласовано иное, временем отправки электронного документа считается время его ввода в информационную систему, не контролируемую лицом, подписавшим или создавшим печать, или посредником электронного документа, отправляющим электронный документ от имени лица, подписавшего или создавшего печать.

(2) Если между лицом, подписавшим или создавшим печать, и адресатом электронного документа не согласовано иное, временем получения электронного документа считается время его ввода в информационную систему, указанную адресатом. Если адресат электронного документа не указал соответствующую информационную систему, электронный документ считается полученным с момента его поступления в информационную систему адресата, а при отсутствии у адресата такой системы - с момента извлечения адресатом электронного документа из информационной системы, через которую он был передан.

(3) Время отправки электронного документа в информационных системах может быть подтверждено, при необходимости, путем нанесения на электронный документ штампа времени.

(4) Если подписант или создатель печати и адресат электронного документа договорились о подтверждении получения электронного документа, то временем получения электронного документа считается время отправки адресатом подтверждения о получении с проставлением в

соответствующих случаях штампа времени.

Статья 49. Ведение учета электронных документов

(1) Электронные записи физических и/или юридических лиц должны храниться в соответствии с законодательством в регистрах.

(2) Электронное делопроизводство включает технологические и программные процедуры заполнения и ведения электронных записей, а также средства хранения электронных документов.

Статья 50. Хранение электронных документов

(1) Субъекты электронного документооборота обязаны хранить оригиналы электронных документов в форме, позволяющей проверить их подлинность.

(2) Срок хранения электронных документов идентичен сроку, установленному законодательством для хранения аналогичных бумажных документов.

(3) Субъекты электронного документооборота могут обеспечить их сохранность, воспользовавшись услугами посредника в электронном документообороте, при условии соблюдения положений настоящего закона.

(4) Электронный архив используется для архивирования электронных документов. Правительство определяет категории электронных документов, для хранения которых используется защищенный электронный архив.

Статья 51. Защита электронных документов

(1) Электронный документ пользуется такой же правовой защитой, как и аналогичный бумажный документ.

(2) Информация, составляющая содержание электронного документа, используется и защищается, согласно закону, в зависимости от ее статуса и степени защиты.

(3) Создание, обработка, отправка, получение, хранение, изменение и/или уничтожение электронного документа должны соответствовать требованиям безопасности, установленным Правительством для систем электронного документооборота юридический лиц публичного права. Требования к безопасности систем электронного документооборота юридических лиц частного права устанавливаются их владельцами.

(4) В процессе создания, обработки, отправки, получения, хранения, изменения и/или уничтожения электронного документа должна сохраняться информация, позволяющая определить происхождение, принадлежность и назначение электронного документа, а также дату его создания, отправки и получения.

Глава V
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ОТВЕТСТВЕННОСТЬ

Статья 52. Защита персональных данных

(1) Поставщики доверительных услуг обеспечат соблюдение законодательства о защите персональных данных в процессе предоставления доверительных услуг.

(2) Личные данные собираются поставщиком доверительных услуг только в объеме, необходимом для выдачи и обслуживания сертификата. Персональные данные не могут собираться или обрабатываться для других целей без прямого согласия субъекта данных.

Статья 53. Ответственность физических и юридических лиц, на которых распространяется действие настоящего Закона

(1) Физические и юридические лица несут ответственность по закону за несоблюдение положений настоящего Закона.

(2) Посредник в электронном документообороте несет ответственность в соответствии с законом за невыполнение или ненадлежащее выполнение обязательств, предусмотренных настоящим законом, за ненадлежащее качество предоставляемых услуг, а также за ущерб, причиненный этими действиями и/или бездействием.

(3) Споры, возникающие в связи с электронным документооборотом , а также связанные с использованием электронных документов и доверительных услуг, разрешаются субъектами электронного документооборота в соответствии с законодательством и заключенными договорами.

Статья 54. Ответственность и бремя доказательства

(1) Поставщик доверительных услуг несет гражданско-правовую ответственность за ущерб, причиненный в результате невыполнения обязательств, предусмотренных настоящим Законом, если только поставщик доверительных услуг не представит соответствующие доказательства того, что он не мог предотвратить причинение ущерба.

(2) Бремя доказывания умысла или халатности неквалифицированного поставщика доверительных услуг лежит на физическом или юридическом лице, требующем компенсации за причиненный ущерб.

(3) Умысел или халатность квалифицированного поставщика доверительных услуг презюмируется, пока не будет доказано обратное.

(4) Поставщики доверительных услуг не несут ответственности за ущерб, возникший в результате использования услуг, превышающих установленные ограничения, если поставщики надлежащим образом

заранее информируют клиентов об ограничениях на использование предоставляемых ими услуг.

Статья 55. Ответственность владельца сертификата открытого ключа

Владелец сертификата открытого ключа несет гражданскую ответственность за ущерб, причиненный в случаях:

a) невыполнение или ненадлежащее выполнение обязательств, предусмотренных настоящим Законом;

b) использование доверенных сервисов, в том числе в период с момента подачи запроса о приостановлении действия или отзыве сертификата открытого ключа до внесения этой записи в реестр сертификатов открытых ключей в установленный срок, если владелец сертификата не предоставит соответствующие доказательства того, что электронный документ подписан другим лицом.

Глава VI
ЗАКЛЮЧИТЕЛЬНЫЕ И ПЕРЕХОДНЫЕ ПОЛОЖЕНИЯ

Статья 56. Заключительные положения

(1) Настоящий закон вступает в силу по истечении 6 месяцев со дня его опубликования в Официальном мониторе Республики Молдова.

(2) В день вступления в силу настоящего закона признаются утратившем силу Закон №91/2014 об электронной подписи и электронном документе (Официальный монитор Республики Молдова, 2014 г., № 174-177, ст. 397) с внесенными в него изменениями.

(3) Правительство, в течение 6 месяцев со дня опубликования настоящего закона:

a) представит в парламент предложения по приведению действующего законодательства в соответствие с этим законом;

b) приведет свои нормативные акты в соответствие с этим законом;

c) разработает и принимает необходимые нормативные акты для реализации настоящего закона.

Статья 57. Переходные положения

(1) Сертификаты открытых ключей, выданные на основании Закона № 91/2014 об электронной подписи и электронном документе остаются действительными до истечения срока их действия.

(2) В течение 12 месяцев со дня вступления в силу настоящего Закона поставщики услуг сертификации открытых ключей, аккредитованные в соответствии с Законом № 91/2014 об электронной подписи и электронном документе, обязаны пройти процедуру аккредитации в соответствии с положениями настоящего Закона.

Если поставщики услуг сертификации открытых ключей, аккредитованные в соответствии с Законом № 91/2014 об электронной подписи и электронном документе не прошли процедуру аккредитации в соответствии с положениями настоящего Закона в срок, установленный части (2), их аттестат аккредитации должен быть отозван.

Председатель Парламента