ПЕРЕВОД

ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ МОЛДОВА

ПОСТАНОВЛЕНИЕ № 1042

от 28 декабря 2013г.

Кишинэу

Об утверждении проекта закона об электронной подписи и электронном документе

Правительство ПОСТАНОВЛЯЕТ:

Утвердить и представить на рассмотрение Парламенту проект закона об электронной подписи и электронном документе.

Премьер-министр **ЮРИЕ ЛЯНКЭ**

Контрасигнуют:

Зам. Премьер-министра,
министр экономики — Валериу ЛАЗЭР

Министр информационных
технологий и связи — Павел Филип

Министр юстиции — Олег Ефрим

Проект
Перевод

ПАРЛАМЕНТ РЕСПУБЛИКИ МОЛДОВА

З А К О Н

Об электронной подписи и электронном документе

Парламент принимает настоящий органический закон

Настоящий закон создает рамки, необходимые для применения Директивы №. 1999/93/ЕС Европейского Парламента и Совета от 13 декабря 1999 года о правовых основах регулирования электронных подписей, опубликованных в Официальном журнале Европейского сообщества №. L 013 от 19 января 2000 года.

Глава I
ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Цель и сфера применения настоящего закона

(1) Настоящий закон устанавливает правовой режим электронной подписи и электронного документа, в том числе основные требования по их действительности и основные требования к сертификационным услугам.

(2) Настоящий закон не ограничивает порядок использования документов.

(3) Признание электронной подписи и электронного документа за пределами Республики Молдова регламентируется международными договорами, одной из сторон которых является Республика Молдова. Если международным договором, одной из сторон которого является Республика Молдова, устанавливаются иные нормы, чем те, которые предусмотрены в настоящем законе, применяются нормы международного договора.

Статья 2. Основные понятия

Для целей настоящего закона используются следующие понятия:

а) *добровольная аккредитация* – авторизация, предусматривающая специальные права и обязанности по предоставлению сертификационных услуг, выданная по запросу поставщика сертификационных услуг компетентным органом по установлению соответствующих прав и обязанностей и контролю над их соблюдением, в случае, когда поставщик сертификационных услуг не наделен полномочиями по осуществлению

прав, вытекающих из разрешения, до получения решения компетентного органа;

b) *подлинность электронного документа* – качество электронного документа, состоящее в подписании его лицом, обладающим подлинной электронной подписью и правом подписи;

c) *защищенный электронный архив* – структурированное хранилище электронных документов, обеспечивающее их конфиденциальность, неотрекаемость и целостность, гарантирующее их доказательную силу во времени;

d) *сертификат открытого ключа* – электронный документ, содержащий открытый ключ, подписанный электронной подписью поставщика сертификационных услуг, подтверждающий принадлежность открытого ключа владельцу сертификата открытого ключа, а также позволяющий идентифицировать данного владельца;

e) *квалифицированный сертификат открытого ключа* – сертификат открытого ключа, удовлетворяющий требованиям, предусмотренным статьей 31 настоящего закона, и выданный поставщиком сертификационных услуг, осуществляющим свою деятельность в соответствии со статьей 26 настоящего закона;

f) *закрытый ключ* – уникальная цифровая последовательность, сформированная при помощи устройства создания подписи и предназначенная для создания электронной подписи;

g) *открытый ключ* – уникальная цифровая последовательность, сформированная при помощи устройства создания подписи, соответствующая независимому закрытому ключу, предназначенная для проверки подлинности электронной подписи;

h) *электронный документооборот* – совокупность процессов создания, обработки, отправления, получения, хранения, изменения и/или уничтожения электронных документов;

i) *данные для создания электронной подписи* – уникальные данные, такие как коды или закрытые ключи, использующиеся подписантом для создания электронной подписи;

j) *данные для проверки электронной подписи* – данные, а также коды или открытые ключи, использующиеся с целью проверки электронной подписи;

k) *устройство создания электронной подписи* – сконфигурированное программное и/или аппаратное обеспечение, использующееся для управления данными для создания подписи;

l) *защищенное устройство создания электронной подписи* – устройство создания электронной подписи, удовлетворяющее требованиям, предусмотренными параграфами 3) и 4) статьи 8 настоящего закона;

m) *устройство проверки электронной подписи* – сконфигурированное программное и/или аппаратное обеспечение, использующиеся для управления данными для проверки подписи;

n) *электронный документ* – информация в электронной форме, создаваемая, структурируемая, обрабатываемая, хранимая и/или передаваемая с помощью компьютера, других электронных устройств, подписанная электронной подписью в соответствии с настоящим законом;

o) *получатель электронного документа* – физическое или юридическое лицо, которому адресован электронный документ, или иное лицо, которое в силу закона или договора получает электронный документ;

p) *посредник в электронном документообороте* – индивидуальный предприниматель или юридическое лицо, которое по поручению составителя и/или получателя электронного документа организует и управляет системой электронного документооборота и/или оказывает услуги, связанные с электронным документооборотом;

q) *метка времени* – атрибут электронного документа, который посредством электронной подписи заверяет, что информация существовала в определенный момент времени с сохранением аутентичности и целостности электронного документа;

r) *поставщик сертификационных услуг* – индивидуальный предприниматель или юридическое лицо, предоставляющее услуги сертификации;

s) *продукт, ассоциированный с электронной подписью* – программное или аппаратное обеспечение или их специфические компоненты, предназначенные для использования поставщиком сертификационных услуг для предоставления сертификационных услуг или с целью создания или проверки электронных подписей;

t) *регистр представительских полномочий на основании электронной подписи* – электронный регистр, в котором регистрируются представительские полномочия на основании электронной подписи, предоставляемые физическими или юридическими лицами иному лицу;

u) *подписчик* – лицо, обладающее устройством создания подписи и действующее как от своего собственного имени, так и от имени физического лица, юридического лица или субъекта, которого оно представляет;

v) *электронная подпись* – данные в электронном виде, прилагаемые или логически связанные с другими электронными данными и использующиеся в качестве способа аутентификации;

w) *сертификационные услуги* – услуги сертификации открытых ключей, проставлению метки времени и иные услуги в области электронной подписи;

x) *система электронного документооборота* – организационно-техническая система, обеспечивающая осуществление электронного документооборота.

Глава II
ПРАВОВОЙ РЕЖИМ ЭЛЕКТРОННОЙ ПОДПИСИ

Статья 3. Принципы использования электронной подписи

Принципами использования электронной подписи являются:

a) свобода выбора и использования любого вида электронной подписи, если требование об использовании конкретного вида электронной подписи в соответствии с областью ее использования не предусмотрено нормативными актами либо соглашением сторон;

b) возможность использования любой технологии и/или технических средств, позволяющих использовать конкретные виды электронных подписей в соответствии с требованиями настоящего закона;

c) недопустимость ссылки на отсутствие юридической силы электронной подписи и/или подписанного ею электронного документа, только на основании того, что такая электронная подпись создана не собственноручно, а с использованием устройства создания подписи и/или продукта, ассоциированного с электронной подписью.

Статья 4. Виды электронных подписей

(1)Видами электронных подписей, принципы и механизмы использования которых, регулируются настоящим законом, являются:

a) простая электронная подпись;

b) усиленная неквалифицированная электронная подпись;

c) усиленная квалифицированная электронная подпись.

(2) Простая электронная подпись – электронная подпись, использующаяся в качестве способа аутентификации, без непосредственной ссылки на подписчика.

(3) Усиленной неквалифицированной электронной подписью является электронная подпись, которая удовлетворяет следующим требованиям:

a) ссылается непосредственно на подписчика;

b) позволяет идентифицировать подписчика;

c) создана при помощи средств, которые могут находиться исключительно под контролем подписчика и

d) связана с данными, к которым она непосредственно относится таким образом, что любое последующее изменение данных может быть обнаружено.

(4) Усиленной квалифицированной электронной подписью является электронная подпись, которая удовлетворяет всем требованиям усиленной неквалифицированной электронной подписи и дополнительно:

a) основывается на квалифицированном сертификате открытого ключа, выданном поставщиком сертификационных услуг, аккредитованным в области применения усиленной квалифицированной электронной подписи;

b) создана с использованием защищенного устройства создания подписи и проверяется защищенно с использованием устройства проверки электронной подписи и/или продукта, ассоциированного с электронной подписью, получившего подтверждение соответствия требованиям, предусмотренным настоящим законом.

Статья 5. Правовой режим использования электронной подписи

(1) Электронная подпись, независимо от имеющейся степени защиты, имеет правовые последствия и принимается в качестве доказательства, в том числе в судопроизводстве, даже если:

a) представляется в электронном виде, или

b) не основывается на сертификате, выданном аккредитованным поставщиком сертификационных услуг, или

c) не основывается на квалифицированном сертификате открытого ключа, или

d) не создана при помощи защищенного устройства создания подписи.

(2) Усиленная квалифицированная электронная подпись имеет такую же юридическую силу, как и собственноручная подпись.

(3) Порядок обеспечения степени защиты усиленной квалифицированной электронной подписи с целью ее уравнения с собственноручной подписью на бумажном носителе определяется компетентным органом в соответствии с полномочиями, предусмотренными в статье 36 параграф (1).

(4) Для электронных подписей, применяемых государственными служащими, Правительство утверждает порядок их применения. Субъекты частного права могут устанавливать более жесткие требования к электронным подписям, применяемым в электронных документах для аутентификации.

(5) Электронная подпись не является средством шифрования информации.

Статья 6. Признание иностранных электронных подписей

(1) Сертификат открытого ключа, выданный поставщиком сертификационных услуг, проживающим или находящимся в другом государстве, признается эквивалентным, с точки зрения правовых

последствий, сертификату открытого ключа, выданному поставщиком сертификационных услуг, проживающим или находящимся в Республике Молдова, в случае если:

a) поставщик сертификационных услуг, проживающий или находящийся в другом государстве, был аккредитован в соответствии с настоящим законом;

b) аккредитованный поставщик сертификационных услуг, проживающий или находящийся в Республике Молдова, гарантирует признание сертификата;

c) сертификат или поставщик сертификационных услуг, выдавший его, признается на основании двустороннего или многостороннего соглашения между Республикой Молдова и другими государствами или международными организациями на основе взаимности.

(2) Электронная подпись и электронный документ, подписанный ею, не могут считаться не имеющими юридической силы только на основании того, что сертификат открытого ключа был выдан в соответствии с законодательством иностранного государства.

Статья 7. Закрытый и открытый ключи

(1) Закрытый и открытый ключи, используемые для создании усиленной неквалифицированной электронной подписи, создаются физическим лицом. Они могут быть созданы третьими лицами с непосредственного согласия соответствующего физического лица при условии обеспечения невозможности их копирования.

(2) Закрытый и открытый ключи, используемые для создания усиленной квалифицированной электронной подписи, создаются поставщиком сертификационных услуг с использованием защищенного устройства создания подписи. В случае использования защищенного устройства создания подписи на базе SIM-карты, поставщик сертификационных услуг обеспечивает физическому лицу инициирование процедуры создания закрытого ключа и открытого ключа.

(3) Создание закрытого ключа и связанного с ним открытого ключа производится одновременно.

(4) Физическое лицо может быть владельцем любого количества закрытых и открытых ключей.

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

(6) Открытый ключ сертифицируется поставщиком сертификационных услуг и является доступным для всех.

Статья 8. Создание электронной подписи

(1) Создание электронной подписи осуществляется посредством устройства создания подписи и/или продукта, ассоциированного с

электронной подписью, с использованием данных для создания электронной подписи.

(2) При создании простой электронной подписи стороны основываются на положениях заключенного соглашения.

(3) При создании усиленной неквалифицированной электронной подписи и усиленной квалифицированной электронной подписи устройство создания подписи и/или продукт, ассоциированный с электронной подписью, должны:

a) обеспечить возможность отображения электронного документа, подписанного электронной подписью, или однозначно ссылаться на подписываемый документ;

b) создавать электронную подпись только после подтверждения подписчиком операции по созданию электронной подписи;

c) однозначно подтверждать создание электронной подписи.

(4) Защищенные устройства создания подписи должны как минимум гарантировать посредством соответствующих технических средств и процедур, что:

a) данные для создания подписи, используемые для создания подписи, появляются только один раз, а их конфиденциальность обеспечивается в соответствии с настоящим законом;

b) данные для создания подписи, использующиеся для создания подписи, не могут быть вычислены, а также что подпись защищена от любой возможной подделки с использованием имеющихся на данное время технологий;

c) данные для создания подписи, использующиеся для создания электронной подписи, должны быть надежно защищены законным подписчиком от их использования другими лицами.

(5) Защищенные устройства создания подписи не должны изменять данные для подписания или препятствовать их визуализации подписчику до процесса подписания.

Статья 9. Проверка подлинности электронной подписи

(1) Проверка подлинности электронной подписи осуществляется при помощи устройства проверки подписи и/или продукта, ассоциированного с электронной подписью, с использованием данных для проверки электронной подписи.

(2) При проверке простой электронной подписи стороны основываются на положениях заключенного соглашения, которое должно предусматривать порядок подтверждения целостности подписанного электронного документа.

(3) При проверке усиленной неквалифицированной электронной подписи и усиленной квалифицированной электронной подписи

устройство проверки подписи и/или продукт, ассоциированный с электронной подписью, должны:

a) обеспечить возможность отображения электронного документа, подписанного электронной подписью, или однозначно ссылаться на подписываемый документ;

b) отображать факт изменения электронного документа, подписанного электронной подписью;

c) ссылаться на подписчика.

(4) При защищенной проверке усиленной неквалифицированной электронной подписи и усиленной квалифицированной электронной подписи с достаточной степенью надежности должно быть гарантировано следующее:

a) соответствие данных, используемых для проверки электронной подписи, данным, отображаемым лицу, проверяющему электронную подпись;

b) надежность проверки электронной подписи и правильность отображения результата проверки и личности подписчика;

c) достоверность проверки подлинности и действительности запрошенного сертификата открытого ключа на момент проверки подписи;

d) четкое отображение содержания сертификата открытого ключа; и

e) возможность обнаружения любых изменений, способных повлиять на защищенность электронной подписи.

Статья 10. Использование простой электронной подписи

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

a) простая электронная подпись содержится в самом электронном документе или логически связана с электронным документом;

b) данные для создания электронной подписи применяются в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и/или отправка электронного документа, и в электронном документе содержится информация, идентифицирующая лицо, от имени которого был создан и (или) отправлен электронный документ.

(2) Нормативные акты и/или соглашение сторон, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать, в частности:

a) правила определения лица, подписывающего электронный документ, по его простой электронной подписи;

b) обязанность лица, создающего и/или использующего данные для создания простой электронной подписи, соблюдать их конфиденциальность.

Статья 11. Ограничения на использование некоторых видов электронных подписей

(1) Не допускается использование простой электронной подписи для усиленной неквалифицированной электронной подписи:

a) подписания электронных документов, содержащих сведения, составляющие государственную тайну;

b) подписания электронных документов в рамках правовых отношений между государственными органами и учреждениями, в том числе подведомственных им структур, с частными физическими и юридическими лицами.

(2) Условия и порядок применения электронной подписи в электронных документах государственных органов и учреждений, в том числе подведомственных им структур, определяются Правительством.

Статья 12. Регистр представительских полномочий на основании электронной подписи

(1) Регистр представительских полномочий на основании электронной подписи содержит данные об уполномоченных лицах, представленных лицах, роль и цель полномочия, даты предоставления полномочий, срок полномочий, другую информацию относительно предоставления, изменения или отзыва полномочий.

(2) Любое изменение в Регистре представительских полномочий на основании электронной подписи относительно делегировании полномочий может быть осуществлено исключительно лицом, предоставляющим данные полномочия.

(3) Правительство определяет владельца и держателя Регистра представительских полномочий на основании электронной подписи, а также порядок его создания и обновления.

Глава III
ПРАВОВОЙ РЕЖИМ ЭЛЕКТРОННОГО ДОКУМЕНТА И ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Статья 13. Правовой режим использования электронного документа

(1) Электронный документ, содержащий усиленную квалифицированную электронную подпись, признается равным по юридической силе с аналогичным документом на бумажном носителе, заверенным собственноручной подписью.

(2) Информация в электронной форме, подписанная простой электронной подписью или усиленной неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, только в случаях, установленных нормативными актами или соглашением сторон по применению электронной подписи, с соблюдением требований, предусмотренных в параграфе (1) статьи 16 настоящего закона.

(3) Нормативные акты или соглашения сторон по применению электронной подписи, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью или усиленной неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи и обязанности сторон в отношении конфиденциальности и материальной ответственности.

(4) Если, согласно законодательству, требуется, чтобы документ был оформлен письменно либо представлен в письменной форме, то электронный документ считается соответствующим этому требованию.

(5) Если, согласно законодательству, требуется, чтобы документ на бумажном носителе был заверен печатью, то электронный документ считается соответствующим этому требованию.

(6) Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан весь пакет электронных документов.

(7) Порядок использования электронных документов в судопроизводстве регламентируется процессуальным законодательством.

(8) Электронный документ признается доказательством, равным по своей значимости письменным доказательствам или вещественным доказательством. Использование электронного документа в качестве доказательства не может быть запрещено по причине его электронной формы.

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

(10) Все одинаковые экземпляры одного электронного документа считаются его оригиналами и имеют одинаковую юридическую силу.

(11) Если определенное лицо создает электронный документ и документ на бумажном носителе, идентичные по содержанию, оба считаются независимыми документами и оригиналами.

(12) Копией электронного документа признается представление (отображение) электронного документа на бумажном носителе в форме,

доступной для восприятия. Копия электронного документа заверяется в порядке, установленном законодательством для заверения копий документов на бумажном носителе, и должна содержать информацию о том, что она является копией электронного документа.

Статья 14. Области и цель использования электронного документа

(1) Электронный документ может использоваться физическими и юридическими лицами во всех сферах деятельности, в которых возможно применение электронных устройств, программных и технических средств, позволяющих создавать, обрабатывать, передавать, принимать, хранить, изменять и/или уничтожать информацию в электронной форме.

(2) Электронный документ может использоваться для передачи данных и сообщений, осуществления переписки, при составлении юридических актов, а также в качестве документа, отражающего экономические факты.

Статья 15. Требования, предъявляемые к электронному документу

Электронный документ должен соответствовать следующим основным требованиям:

a) создаваться, обрабатываться, передаваться, приниматься, храниться, изменяться и/или уничтожаться с помощью программных и/или технических средств;

b) содержать, для подтверждения его подлинности, одну или несколько электронных подписей, соответствующих условиям и требованиям, предусмотренным настоящим законом;

c) создаваться и использоваться способом и в форме, позволяющих идентифицировать подписчика электронного документа;

d) быть отображенным в форме, доступной для восприятия;

e) быть доступным для неоднократного использования.

Статья 16. Подлинность электронного документа

(1) Электронный документ является подлинным, если он соответствует следующим совокупным требованиям:

a) подписан лицом, уполномоченным в установленном порядке подписывать собственноручной подписью подобный документ на бумажном носителе;

b) подписан подлинной электронной подписью подписчика, указанного в документе.

(2) Проверка подлинности электронного документа осуществляется путем проверки, с использованием устройства проверки подписи и/или продукта, ассоциированного с электронной подписью, подлинности этой электронной подписи.

Статья 17. Организация электронного документооборота

(1) Электронный документооборот осуществляется в соответствии с положениями настоящего закона и с правилами, установленными собственником соответствующей системы электронного документооборота, а также с договорами, заключаемыми между субъектами электронного документооборота.

(2) Электронный документооборот может включать:

a) создание и обработку электронного документа;

b) отправку и получение электронного документа;

c) проверку подлинности электронного документа;

d) подтверждение получения электронного документа;

e) учет электронных документов;

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

g) создание дополнительных экземпляров электронного документа;

h) создание и заверение бумажных копий электронного документа;

i) применение метки времени.

(3) Порядок создания, обработки, хранения, отправки, получения, хранения, изменения и/или уничтожения электронного документа в системах электронного документооборота государственных учреждений устанавливается Правительством, а в системах электронного документооборота частных учреждений – их собственниками.

Статья 18. Посредник в электронном документообороте

(1) В организации и осуществлении электронного документооборота могут участвовать посредники в соответствии с положениями настоящего закона и с правилами, установленными собственником соответствующей системы электронного документооборота.

(2) Посредник в электронном документообороте обязан:

a) располагать программными и техническими средствами и/или оборудованием, обеспечивающими надежность и безопасность используемых информационных систем;

b) располагать персоналом, обладающим необходимыми знаниями и/или опытом в области информационных технологий или информационной безопасности;

c) обеспечивать условия точного определения времени и источника отправки электронного документа, а также времени его получения и электронного адреса получателя;

d) обеспечивать защиту и хранение электронных документов;

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

Статья 19. Создание электронного документа

(1) Электронный документ создается его подписчиком и включает информацию, составляющую содержание электронного документа, а также электронную подпись подписчика.

(2) Создание электронного документа завершается применением электронной подписи подписчиком электронного документа, с применением, при необходимости, метки времени.

Статья 20. Отправка и получение электронного документа

(1) Электронный документ может отправляться и приниматься с помощью информационных и телекоммуникационных систем и/или материальных носителей.

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

(3) Если подписчик и получатель электронного документа не согласовали иное, электронный документ считается отправленным, если он:

a) отправлен подписчиком или посредником, действующим от его имени, или информационной системой, используемой подписчиком;

b) надлежащим образом адресован или иным образом направлен в указанную получателем информационную систему;

c) представлен в форме, доступной для обработки в указанной получателем информационной системе;

d) поступает в информационную систему, находящуюся вне контроля подписчика или посредника, который отправляет электронный документ от его имени.

(4) В случае, если подписчик и получатель электронного документа не согласовали иное, электронный документ считается принятым получателем, если он:

a) поступает в информационную систему, из которой получатель способен извлекать электронные документы;

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

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

a) лицо, представленное в документе его подписчиком, в действительности не является таковым;

b) подписчик не является инициатором отправки электронного документа;

c) электронный документ принят получателем в измененном виде или без электронной подписи.

(6) Электронный документ считается неполученным, если лицо, получившее его, в действительности не является его надлежащим получателем.

Статья 21. Момент отправки и получения электронного документа

(1) Если подписчик и получатель электронного документа не согласовали иное, моментом отправления электронного документа считается момент поступления электронного документа в информационную систему, находящуюся вне контроля подписчика или посредника, который отправляет электронный документ от его имени.

(2) Если подписчик и получатель электронного документа не согласовали иное, моментом получения электронного документа считается момент поступления электронного документа в указанную получателем информационную систему. Если получатель электронного документа не указал информационную систему, электронный документ считается полученным им с момента поступления в информационную систему получателя, а в случае отсутствия таковой - с момента его извлечения получателем из информационной системы, посредством которой электронный документ был отправлен.

(3) Момент отправки электронного документа в информационные системы, в случае необходимости, может быть подтвержден применением метки времени в соответствующем электронном документе.

(4) Если соглашением подписчика и получателя электронного документа предусмотрена необходимость подтверждения получения электронного документа, данный документ считается полученным с момента отправления получателем подтверждения о его получении, с применением метки времени, при необходимости.

Статья 22. Учет электронных документов

(1) Учет электронных документов физическими и/или юридическими лицами осуществляется в соответствии с законодательством путем ведения электронных и/или бумажных регистров.

(2) Технология ведения электронных регистров должна включать программно-технологические процедуры заполнения и администрирования электронных регистров, а также средства хранения электронных документов.

Статья 23. Хранение электронных документов

(1) Субъекты электронного документооборота обязаны хранить оригиналы электронных документов на материальных носителях в форме, позволяющей проверять их подлинность.

(2) Срок хранения электронных документов идентичен сроку, предусмотренному законодательством для эквивалентных документов на бумажном носителе.

(3) Субъекты электронного документооборота могут обеспечивать хранение электронных документов, пользуясь услугами посредника в электронном документообороте, при условии соблюдения положений настоящего закона.

(4) Для архивного хранения электронных документов используется электронный архив. Правительство устанавливает категории электронных документов, для хранения которых используется защищенный электронный архив.

Статья 24. Защита электронного документа

(1) Электронный документ пользуется юридической защитой, равной защите аналогичного документа на бумажном носителе.

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

(3) Создание, обработка, отправка, получение, хранение, изменение и/или уничтожение электронного документа должны отвечать требованиям безопасности, установленным Правительством для систем электронного документооборота государственных учреждений. Для систем электронного документооборота частных учреждений, требования безопасности устанавливаются их владельцами.

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

Глава IV
СЕРТИФИКАЦИОННЫЕ УСЛУГИ

Статья 25. Поставщик сертификационных услуг

(1) Поставщики сертификационных услуг в области применения простой электронной подписи и усиленной неквалифицированной подписи имеют право на прохождение процедуры аккредитации. Поставщики сертификационных услуг в области применения усиленной квалифицированной электронной подписи должны быть аккредитованы в обязательном порядке, в соответствии с требованиями настоящего закона.

(2) Поставщики сертификационных услуг организуются иерархически. Во главе иерархии находится поставщик сертификационных услуг высшего уровня.

(3) Поставщики сертификационных услуг в области применения простой электронной подписи и усиленной неквалифицированной подписи организуют самостоятельно иерархию.

(4) Поставщики сертификационных услуг в области применения простой электронной подписи могут создавать один иерархический уровень. Поставщики сертификационных услуг в области применения усиленной неквалифицированной электронной подписи создают два иерархических уровня, в том числе высший уровень.

(5) Организация деятельности поставщиков сертификационных услуг в области применения усиленной квалифицированной электронной подписи, в том числе их иерархия, устанавливается Правительством, в рамках настоящего закона.

(6) Учет аккредитованных поставщиков сертификационных услуг осуществляется компетентным органом в рамках регистра поставщиков сертификационных услуг, постоянно обновляемому и доступ к которому является открытым.

(7) Регистрация в регистре учета поставщиков сертификационных услуг производится компетентным органом в день их аккредитации.

Статья 26. Аккредитация поставщика сертификационных услуг

(1) Аккредитация поставщика сертификационных услуг осуществляется на основании его заявки, адресованной компетентному органу. Аккредитация поставщика сертификационных услуг является бесплатной и предоставляется сроком на 5 лет, если более короткий срок не указан в заявке на аккредитацию.

(2) Аккредитация в области применения усиленной квалифицированной электронной подписи предоставляется поставщику сертификационных услуг, удовлетворяющему следующим требованиям:

a) наличие финансовых ресурсов (банковская гарантия или страховой полис) в сумме не менее 300 тысяч лей для возмещения возможного ущерба, причиненного третьим лицам вследствие их доверия к информации, указанной в сертификате открытого ключа, выданном поставщиком сертификационных услуг, или к информации из регистра сертификатов, выданных поставщиком услуг сертификации;

b) наличие для предоставления сертификационных услуг персонала с высшим образованием в области информационных технологий или информационной безопасности, обладающего знаниями и/или опытом на управленческом уровне, экспертными знаниями в области технологии электронных подписей с соответствующим уровнем защищенности;

c) обеспечение безопасности, надежности и непрерывности сертификационных услуг;

d) обеспечение регистрации информации в регистре сертификатов открытых ключей, в частности оперативное предоставление услуг по приостановлению действия и отзыва сертификата открытого ключа;

e) обеспечение возможности определения точной даты и времени выдачи, приостановления действия или отзыва сертификата открытого ключа;

f) проверка, в соответствии с законодательством, личности человека, которому выдается квалифицированный сертификат открытого ключа;

g) использование систем и продуктов, защищенных от изменений, и гарантирование технической и криптографической безопасности, выполняемых ими функций;

h) создание условий для предотвращения подделки сертификатов и, в случае если поставщик сертификационных услуг генерирует данные для создания подписи, гарантирование конфиденциальности в процессе создания таких данных;

i) использование систем, которые не хранят или копируют данные для создания электронной подписи лица, которому поставщик сертификационных услуг предоставлял услуги по управлению ключами;

k) использование надежных систем для хранения сертификатов в проверяемой форме, таким образом, чтобы:

только авторизованные лица могли вводить и изменять данные;

достоверность информации может быть проверена;

сертификаты могут быть общественно доступными для ознакомления;

любые технические изменения, компрометирующие требования безопасности, должны отображаться оператору.

(3) Поставщики сертификационных услуг в области применения усиленной квалифицированной электронной подписи прилагают к заявке документы, подтверждающие соответствие требованиям, указанным в параграфе (2) настоящей статьи, а именно подтверждают:

a) наличие финансовых ресурсов для восстановления возможного ущерба;

b) наличие внутреннего положения об обеспечении деятельности поставщика сертификационных услуг в соответствии с требованиями настоящего закона;

c) соответствие используемых систем и продуктов требованиям настоящего закона;

d) образование и квалификацию ответственных лиц, чьи функциональные обязанности непосредственно связаны с предоставлением сертификационных услуг;

e) назначение сотрудников, ответственных за деятельность поставщика сертификационных услуг, и лиц, уполномоченных

подписывать сертификаты открытых ключей, а также документы, удостоверяющие личность данных лиц;

f) порядок синхронизации с Всемирным координированным временем (UTC);

g) лицензию, выданную Лицензионной палатой (только для поставщиков, которые предоставляют сертификационные услуги третьим лицам), которая подтверждает право на экспорт, импорт, проектировку, производство и продажу средств криптографической и технической защиты информации, специальных технических средств для скрытого получения информации; предоставление услуг в области криптографической и технической защиты информации (за исключением деятельности органов власти, обладающих этим правом на основании закона).

(4) Указанные в пункте a) параграфа (3) документы представляются в оригинале. Указанные в пунктах b)-g) параграфа 3) документы представляются в оригинале вместе с копией, оригинал возвращается после сверки с копией в момент его предоставления.

(5) При подаче заявки на аккредитацию поставщик сертификационных услуг в области применения простой электронной подписи и усиленной неквалифицированной электронной подписи обязан предоставить информацию в формате, установленном компетентным органом, относительно используемых процедур безопасности и сертификации, а также данные, идентифицирующие его.

(6) Компетентный орган, на основании представленных документов, в течение 30 календарных дней принимает решение об аккредитации поставщика сертификационных услуг или отказе в аккредитации.

(7) В случае принятия решения об аккредитации компетентный орган, в течение 10 календарных дней от момента принятия решения об аккредитации, уведомляет поставщика сертификационных услуг о принятом решении и выдает ему свидетельство об аккредитации установленного образца и, в соответствии с нормативными актами в области электронной подписи, регистрирует аккредитованного поставщика в регистре поставщиков сертификационных услуг.

(8) В случае отказа в аккредитации, компетентный орган, в течение 10 календарных дней с момента принятия решения об отказе, письменно уведомляет поставщика сертификационных услуг о принятом решении с указанием причин отказа.

(9) Основанием для отказа в аккредитации может являться несоответствие поставщика сертификационных услуг требованиям, указанным в параграфе (2) настоящей статьи, или представление недостоверных сведений в документах, прилагаемых к заявке на аккредитацию.

(10) Отказ в аккредитации не может выступать препятствием для повторной подачи документов для аккредитации, сразу после устранения причин, послуживших основанием для отказа в аккредитации.

(11) Решение об отказе в аккредитации может быть обжаловано в судебном порядке.

(12) Поставщик сертификационных услуг считается аккредитованным со дня выдачи свидетельства об аккредитации.

(13) В случае повреждения или утраты свидетельства об аккредитации, в течение 5 рабочих дней со дня подачи соответствующего заявления, поставщику сертификационных услуг выдается дубликат свидетельства.

(14) Информация о поставщиках сертификационных услуг, которые были аккредитованы, а также о тех, аккредитация которых была отозвана, публикуется компетентным органом на его официальной странице в сети Интернет.

(15) После получения свидетельства об аккредитации для предоставления сертификационных услуг в области применения усиленной квалифицированной электронной подписи открытый ключ поставщика сертификационных услуг сертифицируется поставщиком сертификационных услуг высшего уровня, в соответствии с положением, утвержденным компетентным органом.

(16) Аккредитация считается предоставленной или, по обстоятельствам, продленной, если компетентный орган не отвечает заявителю в течение срока, установленного законом для ее выдачи или продления.

(17) По истечении срока, установленного законом для аккредитации и при отсутствии письменного уведомления от компетентного органа, аккредитация считается продленной на 5 лет.

(18) Аккредитованные поставщики сертификационных услуг в области применения простой электронной подписи и усиленной неквалифицированной электронной подписи обязаны уведомить компетентный орган, как минимум за 10 дней до, о любом намерении изменения процедур безопасности и сертификации, с указанием даты и времени когда изменение вступает в силу, и подтвердить в течение 24 часов осуществленное изменения.

(19) В экстренных случаях, в которых безопасность сертификационных услуг находится под угрозой, аккредитованные поставщики сертификационных услуг в области применения простой электронной подписи и усиленной неквалифицированной электронной подписи могут вносить изменения в процедуры безопасности и сертификации, обязуясь проинформировать, в течение 24 часов, компетентный орган об осуществленных изменениях с обоснованием принятого решения.

(20) Аккредитованный поставщик сертификационных услуг обязан обеспечивать соблюдение требований, согласно которым он аккредитован, в течение всего срока его аккредитации. В случае появления обстоятельств, не позволяющих их обеспечение, поставщик сертификационных услуг обязан уведомить об этом компетентный орган в течение 24 часов.

(21) Поставщик сертификационных услуг высшего уровня в области применения усиленной квалифицированной электронной подписи не подлежит аккредитации в соответствии с настоящим законом.

Статья 27. Деятельность поставщика сертификационных услуг

(1) Поставщик сертификационных услуг:

a) создает и выдает сертификаты открытых ключей;

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

c) ведет регистр сертификатов открытых ключей, обеспечивает его обновление и свободный доступ к нему и (или)

d) предоставляет на договорной основе другие услуги, связанные с электронной подписью.

(2) Деятельность поставщика сертификационных услуг представляет собой деятельность в области криптографической и технической защиты информации и подлежит лицензированию Лицензионной палатой, в соответствии с Законом №451-XV от 30 июля 2001 года о регулировании предпринимательской деятельности путем лицензирования.

Статья 28. Обязанности поставщика сертификационных услуг

(1) Поставщик сертификационных услуг обязан:

a) проверять достоверность сведений, указанных в заявке на сертификацию открытого ключа на основании документов, подтверждающих данные сведения;

b) обеспечивать соответствие информации, содержащейся в сертификате открытого ключа информации, представленной владельцем сертификата открытого ключа;

c) включить сертификат открытого ключа в регистр сертификатов открытых ключей не позднее даты и времени начала действия сертификата;

d) обеспечивать доступ к регистру сертификатов открытых ключей, с соблюдением положений статьи 43 настоящего закона;

e) приостанавливать действие или отзывать сертификат открытого ключа в случаях, определенных законом, и вносить соответствующие изменения в регистр сертификатов открытых ключей в установленные сроки;

f) возмещать ущерб, нанесенный любому юридическому или физическому лицу, причиненный вследствие их доверия к информации,

указанной в сертификате открытого ключа в случае, когда была пропущена регистрация отзыва сертификата;

g) уведомлять владельца сертификата открытого ключа о ставших известными поставщику сертификационных услуг фактах, указывающих на невозможность дальнейшего использования закрытого ключа, а также об отзыве сертификата открытого ключа;

h) предоставлять информацию, необходимую для подтверждения подлинности электронной подписи;

i) в случае утраты или повреждения свидетельства об аккредитации, запрашивать выдачу дубликата;

k) осуществлять иные обязанности, установленные настоящим законом.

(2) Поставщик сертификационных услуг, аккредитованный в области применения усиленной квалифицированной электронной подписи обязан, дополнительно:

a) сертифицировать, в установленном законодательством порядке, открытый ключ поставщика сертификационных услуг, аккредитованного в области применения усиленной квалифицированной электронной подписи, предназначенный для сертификации открытых ключей;

b) регистрировать, в соответствующий период времени, в соответствии со статьей 32 настоящего закона, всю необходимую информацию о квалифицированном сертификате открытого ключа, в частности с целью его предоставления в качестве доказательства в суде. Информация может регистрироваться электронными средствами;

c) до вступления в договорные отношения с лицом, запрашивающим сертификат для поддержки его электронной подписи, проинформировать данное лицо, посредством надежных средств связи, о точных сроках и условиях использования сертификата, в том числе об ограничениях по его использованию, о существовании системы аккредитации и процедур рассмотрения исков и урегулирования спорных ситуаций. Такая информация, которая может быть передана в электронном виде, должна быть предоставлена в письменной форме в хорошо читаемом виде. Определенная часть этой информации должна также быть доступна, по требованию, третьим лицам, которые пользуются сертификатом;

d) хранить всю информацию о сертификате открытого ключа, примененному в усиленной квалифицированной электронной подписи, не менее 15 лет с момента отзыва действия или истечения срока действия сертификата, в целях разрешения возможных спорных ситуаций.

Статья 29. Заявка на сертификацию открытого ключа

(1) Заявка на сертификацию открытого ключа подается в электронной форме, подписанная электронной подписью, и/или в виде документа на бумажном носителе, подписанного собственноручной подписью заявителя.

(2) Заявка на сертификацию открытого ключа содержит:

a) фамилию, имя заявителя и номер документа, удостоверяющего личность;

b) другие идентификационные данные заявителя, в зависимости от целей, для которых выдается сертификат открытого ключа, а также сведения, необходимые для обратной связи с заявителем.

Статья 30. Рассмотрение заявки на сертификацию открытого ключа

(1) Заявка на сертификацию открытого ключа рассматривается поставщиком сертификационных услуг в течение 3 рабочих дней с даты регистрации заявки, если стороны не определяют иное.

(2) На основании решения о сертификации открытого ключа поставщик сертификационных услуг создает и выдает соответствующий сертификат открытого ключа. Модель квалифицированного сертификата открытого ключа устанавливается компетентным органом.

(3) Решение об отказе в сертификации открытого ключа принимается поставщиком сертификационных услуг в следующих случаях:

a) нарушения положений настоящего закона;

b) нарушения в процессе подготовки или подачи заявки прав третьих лиц;

c) представления в заявке информации, не соответствующей действительности.

(4) Решение об отказе в сертификации открытого ключа может быть обжаловано в установленном порядке в судебной инстанции.

(5) Решение об отказе в сертификации открытого ключа не лишает заявителя права на подачу новой заявки после устранения всех допущенных нарушений.

Статья 31. Сертификат открытого ключа

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

(2) Сертификат открытого ключа должен содержать следующие сведения:

a) уникальный регистрационный номер сертификата открытого ключа;

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

c) идентификационные данные и другие данные владельца сертификата открытого ключа, в зависимости от цели, для которой выдается сертификат, и сведения, необходимые для обратной связи с ним;

d) открытый ключ;

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

f) данные о криптографическом алгоритме электронной подписи;

g) при необходимости, ограничения на использование сертификата открытого ключа или ограничения стоимости сделок, в которых он может применяться;

h) другие сведения, предусмотренные настоящим законом.

(3) Квалифицированный сертификат открытого ключа выдается аккредитованным поставщиком сертификационных услуг и дополнительно должен содержать следующие сведения:

a) отметку о том, что сертификат выдан в качестве квалифицированного сертификата открытого ключа;

b) возможность включения, по необходимости, специфических особенностей подписчика, в зависимости от цели для которой предназначается данный сертификат;

c) данные для проверки подписи, соответствующие данным для создания подписи под контролем подписчика.

(4) В качестве идентификационных данных владельца сертификата открытого ключа выступают его имя, фамилия и идентификационный номер физического лица (IDNP) и/или псевдоним, в случае использования, а в сертификате открытого ключа поставщика сертификационных услуг - наименование поставщика и идентификационный номер юридического лица (IDNO).

(5) В случае простой электронной подписи и усиленной неквалифицированной электронной подписи структура сертификата открытого ключа определяется поставщиком сертификационных услуг, в соответствии с требованиями настоящего закона. В случае усиленной квалифицированной электронной подписи структура сертификата открытого ключа определяется компетентным органом, в соответствии с требованиями настоящего закона.

(6) Сертификат открытого ключа подписывается электронной подписью поставщика сертификационных услуг, а квалифицированный сертификат открытого ключа подписывается усиленной квалифицированной электронной подписью поставщика сертификационных услуг.

(7) В случаях, установленных законодательством или соглашением сторон, поставщик сертификационных услуг создает сертификат открытого ключа и в виде документа на бумажном носителе в двух экземплярах. В этом случае сертификат открытого ключа в виде документа на бумажном носителе подписывается собственноручными подписями владельца сертификата открытого ключа и уполномоченного лица поставщика услуг сертификации и заверяется печатью поставщика услуг сертификации. Один экземпляр сертификата открытого ключа передается его владельцу, а другой хранится у поставщика сертификационных услуг.

(8) Поставщик сертификационных услуг, по согласованию с владельцем сертификата открытого ключа, может указать в сертификате открытого ключа ограничения по использованию данного сертификата, а также случаи, в которых он может использоваться.

(9) По обращению владельца сертификата открытого ключа поставщик сертификационных услуг может указать в сертификате открытого ключа и другие сведения, не предусмотренные параграфами (2) и (3), при условии, что они не противоречат законодательству, не представляют угрозу безопасности или общественному порядку, и только после предварительной проверки точности этих сведений.

(10) Поставщик сертификационных услуг вносит сертификат в регистр сертификатов открытых ключей не позднее даты и времени начала действия сертификата.

Статья 32. Сроки действия и хранения сертификата открытого ключа

(1) Срок действия сертификата открытого ключа поставщика сертификационных услуг высшего уровня составляет 20 лет, срок действия сертификата открытого ключа поставщика услуг сертификации II уровня составляет 10 лет, срок действия сертификата открытого ключа пользователя устанавливается поставщиком сертификационных услуг, но не может составлять более 1 года.

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

Статья 33. Приостановление действия и отзыв сертификата открытого ключа

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

(2) Поставщик сертификационных услуг отзывает сертификат открытого ключа:

a) по требованию владельца сертификата открытого ключа;

b) при обнаружении недостоверности сведений, указанных в заявке на сертификацию открытого ключа или в сертификате открытого ключа;

c) при нарушении конфиденциальности закрытого ключа (компрометация закрытого ключа);

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

e) при внесении изменений в сертификат открытого ключа;

f) в случае смерти владельца сертификата открытого ключа или признания его недееспособным:

g) по требованию компетентного органа при нарушении данного закона.

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

(4) Поставщик сертификационных услуг обязан уведомить владельца сертификата открытого ключа о причинах отзыва его сертификата.

Статья 34. Обязанности владельца сертификата открытого ключа

Владелец сертификата открытого ключа обязан:

a) обеспечить необходимые условия для исключения доступа другого лица к своему закрытому ключу;

b) не использовать для создания электронной подписи закрытый ключ при имеющихся основаниях полагать, что нарушена конфиденциальность закрытого ключа;

c) незамедлительно требовать приостановления действия или отзыва сертификата открытого ключа в случае:

утери закрытого ключа;

имеющихся оснований полагать, что нарушена конфиденциальность закрытого ключа;

несоответствия действительности информации, содержащейся в сертификате открытого ключа;

d) уведомить, в течение 24 часов, поставщика сертификационных услуг о каких-либо изменениях сведений, содержащихся в сертификате открытого ключа;

e) выполнять другие обязанности, установленные настоящим законом и соглашением с поставщиком услуг сертификации.

Статья 35. Регистр сертификатов открытых ключей

(1) Поставщик сертификационных 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) другую необходимую информацию в соответствии с нормативными актами в области электронной подписи.

(3) В целях осуществления проверки подлинности электронной подписи поставщик сертификационных услуг обязан обеспечивать доступ к регистру сертификатов открытых ключей, в том числе в режиме реального времени.

Глава V
НАДЗОР И КОНТРОЛЬ

Статья 36. Функции органов публичного управления в области применения электронной подписи

(1) Компетентным органом по разработке и реализации государственной политики и контролю в сфере применения всех видов электронной подписи является Служба информации и безопасности Республики Молдова, которая выполняет следующие функции:

a) осуществляет аккредитацию, в том числе добровольную, поставщиков сертификационных услуг;

b) выполняет функции поставщика сертификационных услуг высшего уровня для поставщиков сертификационных услуг, аккредитованных в области применения усиленной квалифицированной электронной подписи;

c) обеспечивает ведение, актуализацию и свободный доступ к данным регистра учета аккредитованных поставщиков сертификационных услуг;

d) разрабатывает и утверждает посредством нормативных актов требования в области применения всех видов электронной подписи;

e) осуществляет надзор и контроль соблюдения требований при оказании услуг по сертификации в области применения всех видов электронной подписи;

f) участвует в разработке и утверждении технических регламентов и стандартов в области электронной подписи;

g) оказывает, по запросу, методическую и практическую помощь органам публичной власти по вопросам применения механизмов электронной подписи;

h) осуществляет международное сотрудничество в области электронной подписи.

(2) Правительство определяет государственный орган или учреждение, ответственное за предоставление услуги единого источника синхронизации со Всемирным координированным временем (UTC).

Статья 37. Контроль в области применения электронной подписи

(1) Компетентный орган следит за соблюдением обязанностей, предусмотренных настоящим законом, при предоставлении сертификационных услуг аккредитованными поставщиками и при предоставлении или продлении аккредитации.

(2) Проверка осуществляется Комиссией по контролю в области электронной подписи (в дальнейшем – Комиссия), на основании Положения, утвержденного компетентным органом.

(3) Комиссия создается в рамках компетентного органа на основании решения руководителя данного органа.

(4) Номинальный состав Комиссии определяется для каждого случая отдельно.

(5) Комиссия имеет право:

a) свободного доступа к документальным материалам, необходимым для проведения работ, на бумажных или электронных носителях, связанных с предоставлением сертификационных услуг, а также к программным дистрибутивам, приложениям и установленным техническим средствам;

b) получать полную информацию об условиях и порядке эксплуатации программных и технических средств;

c) получать информацию от ответственных лиц и персонала поставщика сертификационных услуг в отношении предоставления сертификационных услуг и связанную с предметом контроля;

d) доступа в помещения поставщика сертификационных услуг в течение рабочего дня (на период проведения контроля).

(6) Комиссия не имеет право проводить проверку без наличия приказа о проведение контроля и без документов, удостоверяющих личность членов Комиссии.

(7) При проведении контроля соответствия условиям, предусмотренным настоящим законом, Комиссия руководствуется следующими принципами:

a) законность и соблюдение установленных законом полномочий;

b) недопущение применения не предусмотренных законом санкций;

c) толкование сомнений, возникающих при применении законодательства, в пользу поставщика услуг сертификации;

d) осуществление необходимых для проведения контроля затрат за счет государства;

e) дача рекомендаций для устранения нарушений, установленных в результате контроля;

f) право поставщика сертификационных услуг на обжалование действий органов контроля, в том числе и в судебной инстанции.

(8) Плановые проверки соблюдения поставщиком сертификационных услуг обязательств, предусмотренных настоящим законом, проводятся компетентным органом не чаще одного раза в течение календарного года, с привлечением, при необходимости, представителей регулирующих и контролирующих органов, согласно компетенции.

(9) Планы проверок, разработанные и утвержденные компетентным органом в установленном порядке, согласовываются относительно сроков проведения проверки с руководством поставщика услуг сертификации не позднее, чем за 5 рабочих дней до начала этих проверок.

(10) Внеплановые проверки осуществляется только по решению компетентного органа на основании:

a) установления и подтверждения компетентным органом фактов нарушения данного закона и (или)

b) получения письменных обоснованных заявлений и жалоб в адрес компетентного органа относительно нарушений и ненадлежащего исполнения поставщиком услуг сертификации обязанностей, установленных настоящим законом.

(11) Поставщик сертификационных услуг информируется о проведении внеплановой проверки в день ее начала.

(12) Повторная проверка проводится только с целью проверки выполнения предписаний по устранению нарушений настоящего закона, указанных в акте предыдущей проверки (плановой или внеплановой). Повторная проверка считается составной частью предыдущей проверки.

(13) Проверка проводится в строго указанные приказом о проведении проверки сроки.

(14) Срок осуществления плановой и внеплановой проверки не может превышать 10 рабочих дней, а повторной - не более 5 рабочих дней. В случае внеплановой проверки, срок в 10 дней может быть продлен еще на 10 дней руководителем компетентного органа на основании мотивированного решения, доведенного до сведения контролируемого поставщика сертификационных услуг, которое может быть оспорено поставщиком сертификационных услуг.

(15) При проведении проверки соблюдения обязанностей, установленных настоящим законом, поставщик сертификационных услуг предоставляет сведения и документы относительно цели проверки и не препятствует ее проведению.

(16) По результатам проверки составляется акт в двух экземплярах, один из которых направляется (вручается), не позднее, чем за 5 рабочих дней после завершения проверки, поставщику сертификационных услуг, а второй хранится у компетентного органа. В случае несогласия с результатами проверки поставщик сертификационных услуг, в течение 10 рабочих дней со дня получения акта проверки, может предоставить в письменном виде обоснование несогласия, приложив соответствующие документы.

(17) В случае установления нарушений обязанностей, предусмотренных настоящим законом, компетентный орган, при составлении акта проверки, выдает предписание по устранению нарушений, содержащее рекомендации по устранению всех выявленных нарушений, а также предупреждение о возможном приостановлении действия или отзыве аккредитации в случае неустранения в установленный срок выявленных нарушений.

(18) Минимальный срок, устанавливаемый контролирующим органом для устранения нарушений, составляет 10 рабочих дней, а максимальный - 30 рабочих дней после получения предписания, отправленного (врученного) вместе с актом проверки.

(19) В исключительных случаях, а также по официальному требованию поставщика сертификационных услуг, срок для устранения нарушений может быть продлен до 20 рабочих дней.

(20) Аккредитованный поставщик сертификационных услуг, получив предписание об устранении нарушений обязанностей, предусмотренных настоящим законом, обязан в срок, установленный в предписании, предоставить компетентному органу сведения об устранении нарушений.

(21) При установлении признаков компрометации закрытых ключей аккредитованных поставщиком сертифицированных услуг, нарушения обязанностей, предусмотренных данным законом, немотивированно не устраненных в установленные предписанием сроки, недостоверных данных в сертификатах открытых ключей, компетентный орган вправе применять меры по приостановлению действия или отзыву аккредитации поставщика сертификационных услуг в соответствии с настоящим законом.

(22) Информация о результатах проверки публикуется компетентным органом на его официальной странице в сети Интернет.

(23) Поставщик сертификационных услуг имеет право подавать в письменном виде жалобы по фактам нарушений настоящего закона, допущенных Комиссией, в компетентный орган или оспаривать действия Комиссии в судебной инстанции.

Статья 38. Приостановление и возобновление действия аккредитации.

(1) Действие аккредитации может быть приостановлено в соответствии с Законом № 235-XVI от 20 июля 2006 года об основных принципах регулирования предпринимательской деятельности.

(2) Основанием для осуществления предусмотренных законом мер по приостановлению действия аккредитации, являются:

a) заявление поставщика сертификационных услуг о приостановлении ее действия;

b) нарушение поставщиком сертификационных услуг обязанностей, установленных настоящим законом;

c) недействительность банковской гарантии или страхового полиса, выданного поставщику сертификационных услуг в области применения усиленной квалифицированной электронной подписи, предусмотренных в пункте a) параграфа (2) статьи 26 настоящего закона;

d) невыполнение поставщиком сертификационных услуг предписания по устранению нарушений, установленных в рамках

проверки, проведенной компетентным органом, обязанностей, установленных настоящим законом.

(3) Решение о приостановлении действия аккредитации доводится до сведения поставщика сертификационных услуг в течение 3 рабочих дней со дня его вынесения. Срок приостановления действия аккредитации не может превышать двух месяцев, если нормативными актами в области электронной подписи не предусмотрено иное.

(4) Поставщик сертификационных услуг обязан уведомить в письменном виде компетентный орган об устранении обстоятельств, повлекших приостановление действия аккредитации.

(5) Решение о возобновлении действия аккредитации принимается компетентным органом на основании постановления судебной инстанции, вынесшей решение о приостановлении ее действия, в течение 3 рабочих дней с момента получения уведомления. Решение доводится до сведения поставщика сертификационных услуг в течение 3 рабочих дней со дня его принятия.

(6) Срок действительности аккредитации не продлевается на время приостановления действия ее.

Статья 39. Отзыв аккредитации

(1) Аккредитация может быть отозвана в соответствии с Законом № 235-XVI от 20 июля 2006 года об основных принципах регулирования предпринимательской деятельности.

(2) Основанием для осуществления мер, предусмотренных законом для отзыва аккредитации, являются:

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

b) решение об аннулировании государственной регистрации юридического лица, в рамках которого действует поставщик сертификационных услуг;

c) выявление недостоверных данных в документах, представленных компетентному органу;

d) установление факта передачи свидетельства об аккредитации или его копии другому лицу с целью осуществления аккредитованного вида деятельности;

e) неустранение в установленный срок обстоятельств, повлекших приостановление действия аккредитации;

f) повторное невыполнение предписаний об устранении нарушений, касающихся обязанностей, установленных настоящим законом.

(3) Запись о дате и номере решения об отзыве аккредитации заносится в регистр поставщиков сертификационных услуг не позднее следующего рабочего дня после принятия решения.

(4) Все сертификаты открытых ключей, выданные поставщиком сертификационных услуг в области применения усиленной квалифицированной электронной подписи, прекратившим деятельность, отзываются и передаются на хранение другому поставщику сертификационных услуг в области применения усиленной квалифицированной электронной подписи, в порядке, установленном компетентным органом, за счет прекращающего деятельность поставщика сертификационных услуг.

(5) Поставщик сертификационных услуг обязан, в течение 10 рабочих дней со дня принятия решения об отзыве аккредитации, сдать компетентному органу отозванное свидетельство об аккредитации.

Глава VI
ОТВЕТСТВЕННОСТЬ

Статья 40. Ответственность физических и юридических лиц, подпадающих под действие настоящего закона

(1) Физические и юридические лица несут установленную законодательством ответственность за нарушение положений настоящего закона.

(2) Посредник в электронном документообороте несет установленную законодательством ответственность за неисполнение либо ненадлежащее исполнение обязанностей и ненадлежащее качество оказываемых услуг, а также за ущерб, причиненный вследствие указанных действий (бездействия).

(3) Лица, осуществляющие незаконный доступ к информации, содержащейся в электронных документах, несут гражданскую, административную или уголовную ответственность, в соответствии с законодательством.

(4) Спорные ситуации, возникающие в рамках электронного документооборота, а также связанные с использованием электронных документов и применением электронной подписи, разрешаются между субъектами электронного документооборота в соответствии с законодательством и заключаемыми между ними договорами.

Статья 41. Ответственность поставщика сертификационных услуг

(1) Поставщик сертификационных услуг несет гражданскую, административную или уголовную ответственность, при необходимости, в соответствии с действующими законодательными актами.

(2) Поставщик сертификационных услуг несет гражданскую ответственность за ущерб, причиненный вследствие невыполнения своих обязанностей, предусмотренных настоящим законом, за исключением случаев, когда поставщик сертификационных услуг представляет

соответствующие доказательства того, что он не смог предотвратить процесс причинения убытков.

(3) Поставщик сертификационных услуг не несет гражданской ответственности за убытки, причиненные в связи с использованием сертификата открытого ключа с нарушением ограничений по использованию сертификата или ограничений стоимости сделок, в которых он может использоваться.

Статья 42. Ответственность владельца сертификата открытого ключа

(1) Владелец сертификата открытого ключа несет гражданскую, административную или уголовную ответственность, при необходимости, в соответствии с действующими законодательными актами.

(2) Владелец сертификата открытого ключа несет гражданскую ответственность за ущерб, причиненный вследствие:

a) невыполнения или ненадлежащего выполнения обязанностей, предусмотренных настоящим законом;

b) подписания электронных документов с использованием его закрытого ключа, в том числе в период от требования приостановления действия или отзыва сертификата открытого ключа до внесения в установленный срок соответствующей отметки в регистр сертификатов открытых ключей, за исключением случаев, когда владелец сертификата открытого ключа представляет соответствующие доказательства того, что электронный документ был подписан другим лицом.

Глава VII
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 43. Защита данных персонального характера

(1) Поставщики сертификационных услуг и контролирующий орган обеспечивают соблюдение положений Закона №133 от 8 июля 2011 о защите персональных данных в процессе предоставления услуг сертификации.

(2) Личные данные собираются поставщиком сертификационных услуг, только с предварительного согласия лица, запрашивающего сертификат, и только в случае, когда они необходимы для выпуска и сопровождения сертификата. Персональные данные не могут собираться или обрабатываться для других целей без предварительного и четкого согласия заинтересованного лица.

Глава VIII
ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 44. Заключительные положения

(1) Настоящий закон вступает в силу в течение шести месяцев со дня опубликования.

(2) В день вступления в силу настоящего закона, Закон № 264-XV от 15 июля 2004 года об электронном документе и цифровой подписи признается утратившим силу (Официальный монитор Республики Молдова, 2004 г., № 132-137, ст. 710).

(3) Правительству, в двенадцатимесячный срок с даты опубликования настоящего закона:

a) представить предложения по приведению действующего законодательства в соответствие с настоящим законом;

b) привести свои нормативные акты в соответствие с настоящим законом;

c) разработать и утвердить акты, необходимые для исполнения настоящего закона.

(4) Положения параграфа (1) статьи 5 в части, касающейся судопроизводства, вступают в силу с 1 января 2016 года.

Председатель Парламента

Пояснительная записка
к проекту Закона об электронной подписи и электронном документе

Данная пояснительная записка описывает контекст, в котором разрабатывался проект Закона об электронной подписи и электронном документе (далее – проект закона) и целесообразность проекта закона.

Проект закона создает рамки, необходимые для применения Директивы №. 1999/93/ЕС Европейского Парламента и Совета от 13 декабря 1999 года о правовых основах Сообщества для электронных подписей, опубликованной в Официальном журнале Европейского сообщества №. L 13 от 19.01.2000.

Целью законопроекта является определение правового режима электронной подписи и электронного документа, а также основных требований по их действительности и основных требований к сертификационным услугам. Вместе с тем, законопроект направлен на создание правовых условий для эффективного, безопасного и без необоснованной стоимости использования альтернативных форм аутентификации рукописной подписи.

Интервенция посредством законопроекта обусловлена неэффективностью существующей юридической базы, созданной для цифровой подписи - самой сложной формы электронной подписи. Для упрощения процедур сертификации, выдачи и использования электронных подписей определены несколько видов электронных подписей с различной степенью защиты и юридической значимости и целесообразностью для различных правовых актов.

Законопроектом определяются виды электронных подписей, принципы их использования, правовые последствия использования электронных подписей, а также требования, предъявляемые к поставщикам сертификационных услуг. Законопроект не меняет существующую правовую базу в отношении действительности гражданско-правовых актов, а обеспечивает правовую основу для использования альтернативной аутентификации собственноручной подписи, касающуюся требований к форме для действительности гражданско-правовых актов.

В контексте трансграничного использования электронных подписей, законопроект устанавливает условия, при которых сертификат открытого ключа, выданный поставщиком сертификационных услуг, проживающим или находящимся в другом государстве, признаётся эквивалентным, с точки зрения правовых последствий, сертификату открытого ключа, выданному поставщиком сертификационных услуг, проживающим или находящимся в Республике Молдова, в том числе на основании двустороннего или многостороннего соглашения для признания национальных электронных подписей в других

государствах и признания иностранных электронных подписей в Республике Молдова.

Что касается определений, в целях обеспечения соответствия законопроекта с Директивой №. 1999/93/ЕС, даны определения простой электронной подписи, усиленной неквалифицированной электронной подписи и усиленной квалифицированной электронной подписи. В текст законопроекта были импортированы определения, предоставленные Директивой, относительно устройства создания электронной подписи, защищенного устройства создания электронной подписи, квалифицированных сертификатов открытого ключа, поставщика сертификационных услуг и т.д.

Для обеспечения достаточного уровня защиты документов, подписанных электронной подписью, определено общее правило, согласно которому усиленная квалифицированная электронная подпись приравнивается, с точки зрения юридической значимости, собственноручной подписи. В то же время, Правительство наделяется полномочиями определения порядка применения электронных подписей должностными лицами органов государственной власти. Субъекты частного права могут устанавливать более жесткие требования к электронным подписям, применяемым в электронных документах для аутентификации.

Сферы применения электронных подписей для их признания в судопроизводстве оставлены на усмотрение специального законодательства - гражданско-процессуального. После принятия данного законопроекта потребуется внесение изменений и дополнений в области применения электронных подписей в данном секторе. Предлагается вступление в силу положений, касающихся признания электронных подписей в судопроизводстве, начиная с 2016 года.

Требования к сертификационным услугам, квалификационным сертификатам и к защищенным устройствам создания электронной подписи были переняты целиком из Директивы № 1999/93/ЕС.

Законопроект устанавливает обязательную аккредитацию поставщиков сертификационных услуг в области применения усиленной квалифицированной электронной подписи, а поставщики сертификационных услуг в области применения простой и усиленной неквалифицированной электронной подписи не будут аккредитоваться в обязательном порядке, но смогут пройти процедуру аккредитации по собственной инициативе.

Срок действия сертификата открытого ключа пользователя устанавливается поставщиком сертификационных услуг, но не может составлять более 1 года. Кроме того, установлено обязательство поставщиков сертификационных услуг сохранять, по крайней мере 15 лет, информацию об электронной подписи, чтобы позволить органам уголовного преследования иметь в наличии необходимые

доказательства - в соответствии с Уголовным кодексом, срок исковой давности для тяжких преступлений составляет 15 лет

Законопроект устанавливает компетенцию Службы информации и безопасности по разработке и реализации государственной политики и контролю в сфере применения всех видов электронной подписи.

Реализация закона не потребует дополнительных финансовых затрат из государственного бюджета и будет осуществляться в рамках текущих ассигнований компетентным органам.

Министр **Павел ФИЛИП**