

ЗАКОН РЕСПУБЛИКИ МОЛДОВА
об электронном документе и цифровой подписи

№ 264-XV от 15 июля 2004 г.

Официальный Монитор Республики Молдова № 132-137 от 6 августа 2004 г.

* * *

Парламент принимает настоящий органический закон.

Глава I
Общие положения

Статья 1. Цель и сфера применения настоящего закона

(1) Настоящий закон устанавливает правовые основы использования электронных документов и применения цифровой подписи, определяет основные требования, предъявляемые к электронному документу и цифровой подписи, а также основные правила осуществления электронного документооборота.

(2) Настоящий закон распространяется на отношения, возникающие между физическими и/или юридическими лицами при создании, отправлении, передаче, получении, хранении и ином использовании электронных документов и применении цифровой подписи в любых сферах деятельности, в том числе при совершении сделок, осуществлении платежей и в других предусмотренных законодательством случаях.

(3) Законодательством могут быть установлены ограничения в отношении использования электронных документов и применения цифровой подписи.

Статья 2. Правовая основа

(1) Отношения, возникающие при создании и использовании электронных документов и применении цифровой подписи, регулируются настоящим законом, другими нормативными актами и международными договорами, одной из сторон которых является Республика Молдова, а также соглашениями и договорами между физическими и/или юридическими лицами.

(2) Создание и использование электронного документа, применение цифровой подписи в отношениях, связанных с использованием международных информационных систем или сетей, регламентируется международными договорами, одной из сторон которых является Республика Молдова.

(3) 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 3. Основные понятия

Для целей настоящего закона используются следующие основные понятия:
адресат электронного документа - физическое и юридическое лица или государство, которым направляется электронный документ;

составитель электронного документа - владелец сертификата открытого ключа, создавший электронный документ и подписавший его цифровой подписью;

подлинность электронного документа - качество электронного документа, состоящее в подписании его уполномоченным лицом подлинной цифровой подписью;

подлинность цифровой подписи - качество цифровой подписи, состоящее в подписании электронного документа его составителем с использованием закрытого ключа, соответствующего связанному с ним открытому ключу, использованному при проверке, а также в отсутствие каких-либо изменений в электронном документе после его подписания;

сертификат открытого ключа - электронный документ, содержащий открытый ключ и подписанный цифровой подписью уполномоченного лица

центра сертификации открытых ключей, подтверждающий принадлежность открытого ключа владельцу сертификата открытого ключа, а также позволяющий идентифицировать данного владельца;

закрытый ключ - уникальная цифровая последовательность, сформированная средствами цифровой подписи и предназначенная для создания цифровой подписи;

открытый ключ - уникальная цифровая последовательность, сформированная средствами цифровой подписи, соответствующая связанному с ним закрытому ключу и предназначенная для проверки подлинности цифровой подписи;

электронный документооборот - совокупность процессов создания, обработки, отправления, передачи, получения, хранения, изменения и/или уничтожения электронных документов с применением информационных и телекоммуникационных технологий;

получатель электронного документа - адресат электронного документа или иное лицо, которое в силу закона или договора получает электронный документ, отправленный на имя адресата электронного документа;

электронный документ - информация в электронной форме, создаваемая, структурируемая, обрабатываемая, хранимая, передаваемая с помощью компьютера, других электронных устройств или программных и технических средств, подписанная в соответствии с настоящим законом цифровой подписью;

посредник в электронном документообороте - лицо, которое в установленном порядке или по поручению составителя и/или адресата электронного документа организует и управляет системой электронного документооборота и/или оказывает услуги, связанные с электронным документооборотом;

средства цифровой подписи - программные и/или технические средства, обеспечивающие создание открытого и закрытого ключей, создание цифровой подписи и/или осуществление проверки ее подлинности;

цифровая подпись - неотъемлемый реквизит электронного документа, полученный в результате криптографического преобразования электронного документа с использованием закрытого ключа и предназначенный для подтверждения подлинности электронного документа;

система электронного документооборота - организационно-техническая система, обеспечивающая осуществление электронного документооборота;

материальный носитель - магнитный, оптический, лазерный или иной носитель электронной информации, на котором создается, фиксируется, передается, принимается, хранится или иным образом используется электронный документ и который предоставляет возможность воспроизводить его;

владелец сертификата открытого ключа - физическое лицо, на имя которого центром сертификации открытых ключей выдан сертификат открытого ключа и которое владеет соответствующим закрытым ключом, позволяющим создавать свою цифровую подпись (подписывать электронные документы).

Глава II

Правовой режим электронного документа

Статья 4. Использование электронного документа

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

(2) Электронный документ может использоваться для передачи данных и сообщений, осуществления переписки, при совершении сделок, а также в качестве платежного документа.

Статья 5. Требования, предъявляемые к электронному документу

(1) Электронный документ должен соответствовать следующим основным требованиям:

- а) создаваться, обрабатываться, храниться и передаваться с помощью программных и технических средств;
 - б) содержать реквизиты, позволяющие подтвердить его подлинность, то есть одну или несколько цифровых подписей, соответствующих условиям и требованиям, предусмотренным настоящим законом;
 - с) создаваться и использоваться способом и в форме, позволяющих идентифицировать составителя электронного документа;
 - д) быть представленным (воспроизведенным) в форме, доступной для восприятия человеком;
 - е) быть доступным для его неоднократного использования.
- (2) Требования к содержанию и порядку использования реквизитов электронного документа устанавливаются Правительством и соответствующей системой электронного документооборота.

Статья 6. Юридическая сила электронного документа

- (1) Электронный документ, соответствующий требованиям настоящего закона, признается равным по юридической силе с аналогичным документом на бумажном носителе, заверенным собственноручной подписью.
- (2) Если согласно законодательству требуется, чтобы документ был оформлен письменно либо представлен в письменной форме, то электронный документ считается соответствующим этому требованию.
- (3) Если согласно законодательству требуется, чтобы документ на бумажном носителе был заверен печатью, то электронный документ не требует такого заверения.
- (4) Порядок использования электронных документов в судебной системе регламентируется процессуальным законодательством.
- (5) Электронный документ признается доказательством, равным по своей значимости письменным доказательствам. Использование электронного документа в качестве доказательства не может быть запрещено по причине его электронной формы.
- (6) Если законодательством предусмотрена государственная регистрация документа, то государственной регистрации подлежит оригинал электронного документа.
- (7) Электронный документ не требует нотариальной заверки, если иное не предусмотрено законом.

Статья 7. Оригинал и копия электронного документа

- (1) Все одинаковые экземпляры одного электронного документа считаются его оригиналами и имеют одинаковую юридическую силу.
- (2) В случае, когда одним лицом создаются одинаковые по содержанию электронный документ и документ на бумажном носителе, оба документа признаются самостоятельными документами и являются оригиналами.
- (3) Копией электронного документа признается представление (отображение) электронного документа на бумажном носителе в форме, доступной для восприятия человеком. 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 8. Подлинность электронного документа

- (1) Электронный документ является подлинным, если он:
 - а) подписан лицом, уполномоченным в установленном порядке подписывать собственноручной подписью подобный документ на бумажном носителе;
 - б) подписан подлинной цифровой подписью составителя, указанного в документе.
- (2) Проверка подлинности электронного документа осуществляется путем проверки подлинности цифровой подписи средствами цифровой подписи.

Глава III Электронный документооборот

Статья 9. Организация электронного документооборота

- (1) Электронный документооборот осуществляется в соответствии с

положениями настоящего закона, других нормативных актов и с правилами 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) отправление, передачу и получение электронного документа;
- c) проверку подлинности электронного документа;
- d) подтверждение получения электронного документа;
- e) отзыв электронного документа;
- f) учет электронного документа;
- g) хранение, изменение и уничтожение электронного документа;
- h) создание дополнительных экземпляров электронного документа;
- i) создание и заверение бумажных копий электронного документа.

(3) Требования к осуществлению электронного документооборота в органах публичной власти устанавливаются Правительством.

Статья 10. Субъекты электронного документооборота

(1) Субъектами электронного документооборота могут быть:

- a) граждане Республики Молдова, иностранные граждане и лица без гражданства;
- b) юридические лица, в том числе иностранные, независимо от вида собственности и организационно-правовой формы;
- c) государство в лице органов публичной власти;
- d) международные организации;
- e) посредники в электронном документообороте;
- f) центры сертификации открытых ключей.

(2) Субъекты электронного документооборота наделяются правами и обязанностями, установленными законодательством и соответствующими договорами.

Статья 11. Посредник в электронном документообороте

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

(2) Посредник в электронном документообороте обязан:

- a) располагать программными и техническими средствами и оборудованием, обеспечивающими надежность и безопасность используемых информационных систем;
- b) располагать персоналом, обладающим необходимыми знаниями, опытом и квалификацией;
- c) обеспечивать условия точного определения времени и источника отправления и передачи электронного документа, а также времени и адреса его получения;
- d) использовать надежные системы защиты и хранения электронных документов;
- e) хранить электронные документы в соответствии с договором с составителем и/или адресатом электронного документа.

Статья 12. Создание и формы представления электронного документа

(1) Электронный документ создается составителем электронного документа и включает информацию в соответствующем формате, составляющую содержание электронного документа, а также цифровую подпись составителя и другие установленные реквизиты.

(2) Создание электронного документа завершается его подписанием составителем электронного документа цифровой подписью.

(3) Электронный документ имеет формы внутреннего и внешнего представления (отображения).

(4) Формой внутреннего представления электронного документа является запись информации, составляющей электронный документ, в электронной форме.

(5) Формой внешнего представления электронного документа является воспроизведение электронного документа на экране компьютера, на бумажном

и ином материальном носителе в форме, доступной для восприятия человеком.

Статья 13. Отправление и получение электронного документа

(1) Электронный документ может отправляться, передаваться и приниматься с помощью автоматизированных информационных, телекоммуникационных, информационно-телекоммуникационных систем, средств связи, сетей и материальных носителей, если иное не предусмотрено законом.

(2) Электронный документ должен отправляться и передаваться в форме, позволяющей адресату электронного документа хранить и воспроизводить его.

(3) Если иное не согласовано составителем и адресатом электронного документа, электронный документ считается отправленным, если он:

а) отправлен составителем или посредником, действующим от его имени, или автоматизированной информационной системой, используемой составителем;

б) надлежащим образом адресован или иным надлежащим образом направлен в указанную адресатом автоматизированную информационную систему;

с) представлен в форме, доступной для обработки в указанной адресатом автоматизированной информационной системе;

д) поступает в автоматизированную информационную систему, находящуюся вне контроля составителя или посредника, который отправляет электронный документ от его имени.

(4) Если иное не согласовано составителем и адресатом электронного документа, электронный документ считается полученным адресатом, если он:

а) поступает в указанную адресатом автоматизированную информационную систему, из которой адресат способен извлекать электронные документы;

б) поступает в указанную адресатом автоматизированную информационную систему в форме, доступной для его обработки данной системой.

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

а) лицо, представленное в документе его составителем, в действительности не является таковым;

б) составитель не является инициатором отправления электронного документа;

с) электронный документ получен адресатом в измененном виде или без цифровой подписи.

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

Статья 14. Момент отправления и получения электронного документа

(1) Если иное не согласовано составителем и адресатом электронного документа, моментом отправления электронного документа считается момент поступления электронного документа в автоматизированную информационную систему, находящуюся вне контроля составителя или посредника, который отправляет электронный документ от его имени.

(2) Если иное не согласовано составителем и адресатом электронного документа, моментом получения электронного документа считается момент поступления электронного документа в указанную адресатом автоматизированную информационную систему. Если адресат электронного документа не указал информационную систему, электронный документ считается полученным им с момента поступления в автоматизированную информационную систему адресата, а если адресат не имеет автоматизированной информационной системы – с момента его извлечения адресатом из автоматизированной информационной системы, в которую поступил электронный документ.

(3) Если приглашением составителя и адресата электронного документа предусмотрена необходимость подтверждения получения электронного документа, данный документ считается полученным с момента отправления адресатом подтверждения о его получении.

Статья 15. 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 16. 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 не должен быть меньше срока, предусмотренного законодательством для подобных документов на бумажном носителе.

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

(4) Создание архивов электронных документов, передача электронных документов в архивные учреждения и их хранение в данных учреждениях осуществляются в порядке, установленном Правительством.

Статья 17. 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 правового статуса.

(3) Создание, обработка, отправление, передача, получение и хранение электронного документа должны отвечать установленным требованиям безопасности, предъявляемым к конкретной автоматизированной информационной системе. Требования к безопасности определенных видов информационных систем устанавливаются Правительством.

(4) В процессе обработки, отправления, передачи, получения и хранения электронного документа должна храниться также информация, позволяющая установить происхождение, принадлежность и назначение электронного документа, а также дату его создания, отправления, передачи и получения.

Глава IV

Правовой режим цифровой подписи

Статья 18. Порядок применения цифровой подписи

(1) Электронный документ подписывается цифровой подписью лица, уполномоченного в соответствии с законодательством или договором подписывать собственноручной подписью подобный документ на бумажном носителе.

(2) Цифровая подпись создается владельцем сертификата открытого ключа средствами цифровой подписи с использованием закрытого ключа.

(3) Порядок применения цифровой подписи в электронных документах органов публичной власти устанавливается Правительством.

Статья 19. Юридическая сила цифровой подписи

(1) Цифровая подпись юридически равнозначна собственноручной подписи в документе на бумажном носителе при условии:

а) подлинности цифровой подписи, подтвержденной сертифицированными средствами цифровой подписи, и

б) действительности на момент подписания электронного документа сертификата открытого ключа, составленного и выданного в установленном законодательством порядке.

(2) Цифровая подпись признается равной по юридической силе собственноручной подписи в документе на бумажном носителе, заверенной печатью при наличии полномочий на использование печати.

(3) Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, может заверяться цифровой подписью уполномоченного лица. В данном случае оригиналом считается документ на бумажном носителе.

Статья 20. Проверка подлинности цифровой подписи
Проверка подлинности цифровой подписи осуществляется сертифицированными средствами цифровой подписи с использованием сертификата открытого ключа составителя, подписавшего электронный документ.

Статья 21. Закрытый и открытый ключи

- (1) Закрытый и открытый ключи создаются физическими лицами.
- (2) Физическое лицо самостоятельно создает закрытый и открытый ключи с применением средств цифровой подписи.
- (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 центром сертификации открытых ключей и является доступным для всех субъектов электронного документооборота.

Статья 22. Средства цифровой подписи

- (1) Средства цифровой подписи не являются средствами шифрования информации и подлежат обязательной сертификации в соответствии с законодательством о сертификации товаров и услуг.
- (2) Средства цифровой подписи должны обеспечить:
 - а) уникальность создаваемых закрытого и открытого ключей;
 - б) необходимую вычислительную сложность определения закрытого ключа и цифровой подписи;
 - в) конфиденциальность закрытого ключа.

Глава V

Сертификация открытых ключей

Статья 23. Центр сертификации открытых ключей

- (1) Центром сертификации открытых ключей является юридическое лицо или подразделение юридического лица, оказывающее услуги по сертификации открытых ключей и иные виды услуг, связанные с цифровой подписью.
- (2) Деятельность центров сертификации открытых ключей, оказывающих услуги по сертификации открытых ключей, является деятельностью в сфере криптографической защиты информации и подлежит лицензированию в соответствии с законодательством.
- (3) Центры сертификации открытых ключей организуются иерархически. Во главе иерархии находится центр сертификации высшего уровня.
- (4) Порядок создания и организации деятельности центров сертификации открытых ключей, их подчиненность, а также требования, предъявляемые к финансовым ресурсам центров сертификации, устанавливаются Правительством.
- (5) Учет центров сертификации открытых ключей осуществляется в рамках Государственного регистра правовых единиц.

Статья 24. Лицензирование деятельности центра сертификации открытых ключей

- (1) Деятельность центров сертификации открытых ключей, предоставляющих третьим лицам услуги по сертификации открытых ключей, а также по удостоверению копий электронных документов на бумажном носителе, подлежит лицензированию в соответствии с законодательством.
- (2) Деятельность центров сертификации открытых ключей органов публичного управления, а также юридических лиц, созданных в корпоративных целях и не предоставляющих услуг по сертификации открытых ключей третьим лицам, не лицензируется.

Статья 25. Деятельность центра сертификации
открытых ключей

(1) Центр сертификации открытых ключей:

- a) создает и выдает сертификаты открытых ключей;
- b) приостанавливает и возобновляет действие сертификатов открытых ключей, а также отзывает их;
- c) ведет реестр сертификатов открытых ключей, обеспечивает его актуализацию и свободный доступ к нему;
- d) оказывает на договорной основе иные виды услуг, связанные с цифровой подписью.

(2) Для предоставления услуг по сертификации открытых ключей центры сертификации открытых ключей должны соответствовать следующим условиям:

- a) обладать соответствующими финансовыми, материальными, техническими и социальными ресурсами для обеспечения безопасности, надежности и непрерывности предоставляемых услуг по сертификации открытых ключей, а также для покрытия ущерба, который они могли бы нанести в связи с предоставлением данных услуг;
- b) сертифицировать открытый ключ уполномоченного лица центра сертификации, предназначенный для сертификации открытых ключей, в установленном законодательством порядке;
- c) обеспечивать надежную и оперативную регистрацию информации в реестре сертификатов открытых ключей, в частности оперативное предоставление услуг по приостановлению действия и отзыву сертификатов открытых ключей;
- d) обеспечивать возможность определения даты и времени выдачи, приостановления действия или отзыва сертификата открытого ключа;
- e) располагать персоналом, обладающим квалификацией, необходимой для предоставления услуг по сертификации открытых ключей;
- f) принимать необходимые меры по обеспечению безопасности и защите информации, а также соблюдать требования законодательства;
- g) хранить всю информацию о сертификате открытого ключа не менее десяти лет с момента отзыва сертификата на случай возникновения спора;
- h) соответствовать другим специальным условиям, установленным уполномоченным органом.

(3) Основные требования по обеспечению безопасности информационных и телекоммуникационных систем центров сертификации, использованию ими средств криптографической и технической защиты информации устанавливаются уполномоченным органом.

Статья 26. Обязанности центра сертификации
открытых ключей

Центр сертификации открытых ключей обязан:

- a) убедиться в достоверности данных, указанных в заявке на сертификацию открытого ключа, на основании документов, подтверждающих указанные данные;
- b) обеспечить соответствие информации, содержащейся в сертификате открытого ключа, информации, представленной владельцем сертификата открытого ключа;
- c) включить сертификат открытого ключа в реестр сертификатов открытых ключей не позднее даты и времени начала действия сертификата;
- d) обеспечить свободный доступ к реестру сертификатов открытых ключей;
- e) приостановить действие сертификата открытого ключа или отозвать его в случаях, определенных законом, и внести соответствующие изменения в реестр сертификатов открытых ключей в установленные сроки;
- f) уведомить владельца сертификата открытого ключа о ставших известными центру сертификации фактах, указывающих на невозможность дальнейшего использования закрытого ключа, а также об отзыве сертификата открытого ключа;
- g) предоставлять имеющуюся информацию, необходимую для подтверждения подлинности цифровой подписи;
- h) осуществлять иные обязанности, установленные настоящим законом и другими нормативными актами.

Статья 27. Прекращение деятельности центра сертификации открытых ключей

(1) Деятельность центра сертификации открытых ключей может быть прекращена в установленном законодательством порядке, в том числе по инициативе уполномоченного органа, при нарушении законодательства о цифровой подписи.

(2) Все сертификаты открытых ключей, выданные центром сертификации открытых ключей, деятельность которого прекращена, отзываются и передаются на хранение в установленном законодательством порядке за счет центра сертификации, прекращающего свою деятельность.

Статья 28. Заявка на сертификацию открытого ключа

(1) Заявка на сертификацию открытого ключа составляется в форме электронного документа и подписывается с использованием закрытого ключа, связанного с сертифицируемым открытым ключом.

(2) В случаях, установленных законодательством или соглашением сторон, заявка составляется и в виде документа на бумажном носителе, подписанного собственноручной подписью лица.

(3) Заявка на сертификацию открытого ключа должна содержать:

- a) фамилию и имя физического лица, номер документа, удостоверяющего личность;
- b) другие идентификационные данные лица в зависимости от целей, для которых выдается сертификат открытого ключа, а также информацию, необходимую для передачи ему сообщений;
- c) сертифицируемый открытый ключ;
- d) другие сведения, установленные уполномоченным органом.

Статья 29. Рассмотрение заявки на сертификацию открытого ключа

(1) Заявка на сертификацию открытого ключа рассматривается центром сертификации открытых ключей в течение трех дней, начиная с даты регистрации заявки, после чего центр принимает решение о сертификации либо об отказе в сертификации открытого ключа.

(2) На основании решения о сертификации открытого ключа центром сертификации открытых ключей создается и выдается соответствующий сертификат открытого ключа установленного образца.

(3) Решение об отказе в сертификации открытого ключа принимается центром сертификации открытых ключей в случае:

- a) нарушения положений настоящего закона и других нормативных актов о цифровой подписи;
- b) нарушения в процессе составления 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 компетентную судебную инстанцию.

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

Статья 30. Сертификат открытого ключа

(1) При создании сертификата открытого ключа центр сертификации открытых ключей обязан проверить уникальность открытого ключа.

(2) Сертификат открытого ключа должен содержать следующие сведения:

- a) отдельный регистрационный номер сертификата открытого ключа;
- b) идентификационные данные центра сертификации открытых ключей, выдавшего сертификат открытого ключа;
- c) фамилию и имя владельца сертификата открытого ключа;
- d) другие идентификационные данные владельца сертификата открытого ключа в зависимости от целей, для которых выдается сертификат, а также информацию, необходимую для передачи ему сообщений;
- e) открытый ключ;
- f) даты и время начала и окончания срока действия сертификата открытого ключа;
- g) данные о криптографическом алгоритме цифровой подписи;

h) при необходимости - ограничения по использованию сертификата открытого ключа или ограничения стоимости сделок, в которых он может использоваться;

i) другие сведения, установленные уполномоченным органом.

(3) Сертификат открытого ключа подписывается цифровой подписью уполномоченного лица центра сертификации открытых ключей.

(4) В случаях, установленных законодательством или соглашением сторон, центр сертификации открытых ключей 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 центра сертификации открытых ключей и заверяется печатью центра сертификации. Один экземпляр сертификата открытого ключа передается его владельцу, а другой хранится в центре сертификации.

(5) Центр сертификации открытых ключей 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.

(6) По обращению владельца сертификата открытого ключа центр сертификации открытых ключей может указать в сертификате открытого ключа и другие сведения, не предусмотренные частью (2), при условии, что они не противоречат законодательству, не представляют угрозу безопасности или общественному порядку, и только после предварительной проверки точности этих сведений.

(7) Центр сертификации открытых ключей вносит сертификат в реестр сертификатов открытых ключей не позднее даты и времени начала действия сертификата.

Статья 31. Сроки действия и хранения сертификата открытого ключа

(1) Срок действия сертификата открытого ключа устанавливается центром сертификации открытых ключей, но не может составлять более пяти лет.

(2) Центр сертификации открытых ключей обязан хранить сертификат открытого ключа не менее десяти лет с момента отзыва сертификата.

Статья 32. Отзыв сертификата открытого ключа

(1) Центр сертификации обязан отозвать сертификат открытого ключа в следующих случаях:

- a) по истечении срока действия сертификата открытого ключа;
- b) по требованию владельца сертификата открытого ключа;
- c) при обнаружении недостоверности сведений, указанных в заявке на сертификацию открытого ключа или в сертификате открытого ключа;
- d) при нарушении конфиденциальности закрытого ключа (компрометация закрытого ключа);
- e) по решению уполномоченного органа;
- f) по истечении срока, на который было приостановлено действие сертификата открытого ключа;
- g) при внесении изменений в сертификат открытого ключа;
- h) в случае смерти владельца сертификата открытого ключа или признания его недееспособным;

i) в других установленных уполномоченным органом случаях согласно процедурам обеспечения безопасности и сертификации открытых ключей.

(2) При получении информации о необходимости отзыва сертификата открытого ключа центр сертификации открытых ключей обязан в течение трех рабочих часов внести соответствующие изменения в реестр сертификатов открытых ключей.

(3) Центр сертификации открытых ключей по первому требованию владельца сертификата открытого ключа обязан уведомить его о причинах отзыва сертификата.

Статья 33. 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 цифровой 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 содержащейся в сертификате открытого ключа информации действительности;
- d) своевременно уведомлять центр сертификации открытых ключей о каких-либо изменениях информации, содержащейся в сертификате открытого ключа;
- e) выполнять другие обязанности, установленные настоящим законом и соглашением с центром сертификации открытых ключей.

Статья 34. Реестр сертификатов открытых ключей

- (1) Центр сертификации открытых ключей обязан вести реестр сертификатов открытых ключей.
- (2) Реестр сертификатов открытых ключей должен содержать:
 - a) действительные сертификаты открытых ключей;
 - b) отозванные сертификаты открытых ключей;
 - c) дату и время выдачи сертификатов открытых ключей;
 - d) дату и время отзыва сертификатов открытых ключей;
 - e) другую необходимую информацию.
- (3) В целях осуществления проверки подлинности цифровой подписи центр сертификации открытых ключей обязан обеспечивать свободный доступ к реестру сертификатов открытых ключей, в том числе в режиме реального времени.

Статья 35. Признание сертификатов открытых ключей, выданных центрами сертификации открытых ключей других государств

Сертификат открытого ключа, выданный центром сертификации открытых ключей другого государства в соответствии с законодательством данного государства, признается равнозначным сертификату открытого ключа, выданному центром сертификации открытых ключей Республики Молдова, на основании двусторонних или многосторонних соглашений между Республикой Молдова и другими государствами или международными организациями на взаимной основе.

Глава VI Государственный контроль

Статья 36. Функции органов публичного управления в области использования электронных документов и сфере применения цифровой подписи

- (1) Разработка и реализация государственной политики, а также контроль в области использования электронных документов осуществляются органами публичного управления в пределах их компетенции.
- (2) Уполномоченным органом по разработке и реализации государственной политики и контролю в сфере применения цифровой подписи является Служба информации и безопасности Республики Молдова, которая выполняет следующие функции:
 - a) разрабатывает и утверждает требования в сфере применения цифровой подписи;
 - b) осуществляет мониторинг и контроль за обеспечением требований безопасности при оказании услуг по сертификации открытых ключей;
 - c) участвует в разработке и утверждении стандартов в сфере применения цифровой подписи;
 - d) оказывает методическую и практическую помощь органам публичной власти по вопросам применения механизмов цифровой подписи;

- e) обеспечивает функционирование центра сертификации открытых ключей высшего уровня;
- f) представляет данные о центрах сертификации открытых ключей для внесения в Государственный регистр правовых единиц;
- g) создает и управляет системой сертификации средств цифровой подписи;
- h) осуществляет международное сотрудничество в сфере применения цифровой подписи;
- i) выполняет другие функции, предусмотренные законодательством.

Статья 37. Контроль в сфере применения цифровой подписи

(1) При осуществлении контроля в сфере применения цифровой подписи уполномоченный орган вправе:

- a) проверять исполнение центрами сертификации открытых ключей требований по обеспечению безопасности при оказании услуг по сертификации открытых ключей;
- b) требовать и получать свободный и постоянный доступ в здания и на территорию центров сертификации открытых ключей, к информации и документам, касающимся оказания услуг по сертификации открытых ключей;
- c) безвозмездно получать необходимую для проведения контроля информацию;
- d) в случае выявления нарушений законодательства при необходимости приостанавливать деятельность центра сертификации открытых ключей на срок до 30 дней;
- e) предпринимать иные меры в соответствии с законодательством.

(2) При грубом нарушении центром сертификации открытых ключей требований законодательства о цифровой подписи или неустранении в установленный срок выявленных нарушений уполномоченный орган вправе инициировать принятие решения о прекращении деятельности центра сертификации.

Глава VII

Ответственность

Статья 38. Ответственность физических и юридических лиц

(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 обязан возместить убытки, причиненные вследствие указанных действий (бездействия).

(3) Лица, осуществляющие незаконный доступ к информации, содержащейся в электронных документах, несут ответственность в соответствии с законодательством о доступе к информации.

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

Статья 39. Ответственность центра сертификации открытых ключей

(1) Центр сертификации открытых ключей несет ответственность за убытки, причиненные вследствие невыполнения своих обязанностей, предусмотренных настоящим законом, за исключением случаев, когда центр сертификации представляет доказательства того, что он не смог предотвратить причинение убытков.

(2) Центр сертификации открытых ключей не несет 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 40. Ответственность владельца
сертификата открытого ключа

Владелец сертификата открытого ключа несет ответственность за убытки, причиненные вследствие:

- a) невыполнения обязанностей, предусмотренных настоящим законом;
- b) подписания электронных документов с использованием его закрытого ключа другими лицами, в том числе в период от требования приостановления действия или отзыва сертификата открытого ключа до внесения в установленный срок соответствующей отметки в реестр сертификатов открытых ключей, за исключением случаев, когда владелец сертификата открытого ключа представляет доказательства того, что электронный документ был подписан другим лицом.

Глава VIII
Заключительные положения

Статья 41

Настоящий закон вступает в силу по истечении трех месяцев со дня опубликования.

Статья 42

(1) Правительству в трехмесячный срок:

- a) представить Парламенту предложения по приведению действующего законодательства в соответствие с настоящим законом;
- b) привести свои нормативные акты в соответствие с настоящим законом;
- c) обеспечить приведение ведомственных нормативных актов в соответствие с настоящим законом.

(2) Службе информации и безопасности Республики Молдова:

- a) создать и обеспечить функционирование центра сертификации открытых ключей высшего уровня и центра сертификации открытых ключей органов публичной власти;
- b) разработать нормативные акты, необходимые для обеспечения исполнения настоящего закона.

(3) Национальному банку Молдовы осуществлять контроль над платежным электронным документооборотом и применением цифровой подписи в банковском секторе и других платежных системах.

ПРЕДСЕДАТЕЛЬ
ПАРЛАМЕНТА

Еуджениа ОСТАПЧУК

Кишинэу, 15 июля 2004 г.
№ 264-XV