

?Закон об электронных документах?

Латвийской Республики. Неофициальный перевод Александра Щербина от 26 октября 2006 года. Текст первоисточника – <HTTP: doc.php?id="68521" www.likumi.lv>

?Закон об электронных документах? от 31.10.2002 ("LV", 169 (2744), 20.11.2002) [в силе с 01.01.2003] с изменениями:

- закон ("LV", 75 (3023), 13.05.2004.) от 06.05.2004
- закон ("LV", 178 (3126), 10.11.2004.) от 28.10.2004
- закон ("LV", 107 (3475), 07.07.2006.) от 22.06.2006

Редакции: [01.01.2003] [27.05.2004] [20.08.2004] [24.11.2004] [04.05.2006] [21.07.2006]

Редакция закона от 21.07.2006.

Саэим принял и президент государства провозгласил следующий закон:

## Закон об электронных документах

### Раздел I

#### Общие положения

#### 1 статья. Термины, использованные в законе

В законе используются следующие термины:

- 1) средства создания безопасной электронной подписи – программное обеспечение, аппаратура и данные для создания электронной подписи, которые отвечают следующим требованиям:
  - a) данные для создания электронной подписи созданы только один раз и обеспечена их секретность,
  - b) данные для создания электронной подписи нельзя скопировать, и, используя технологии, электронная подпись защищена от подделки,
  - c) данные для создания электронной подписи надежно защищены от незаконного

- использования их третьим лицом,
- d) средства создания безопасной электронной подписи не изменяют подписываемый документ и не запрещают ознакомиться с этим документом перед его подписанием;
- 2) безопасная электронная подпись – электронная подпись, которая отвечает всем таким требованиям:
- a) она связана только с подписывающим лицом,
- b) она обеспечивает идентификацию подписывающего лица,
- c) она создана средствами создания безопасной электронной подписи, которые может контролировать только подписывающее лицо,
- d) она связана с подписанным электронным документом таким образом, чтобы последующие изменения этого документа были бы заметны,
- e) она подтверждена квалификационным сертификатом;
- 3) электронный документ – любые данные, которые созданы, сохранены, отправлены или приняты электронным способом и которые обеспечивают возможность использовать их для ведения какой-либо деятельности, осуществления прав и защиты;
- 4) электронная подпись – электронные данные, которые приложены к электронному документу или логически связаны с этим документом и которые обеспечивают аутентичность документа и подтверждают идентификацию подписывающего лица;
- 5) проверочные данные электронной подписи – данные, которые используют для проверки электронной подписи;
- 6) данные для создания электронной подписи – только один раз созданные данные, которые использует подписывающее лицо для создания электронной подписи;
- 7) квалификационный сертификат – сертификат, который содержит информацию, оговоренную в этом законе и который выдан

доверительным поставщиком  
сертификационных услуг;

8) временная печать – электронно-  
подписанное подтверждение того, что  
электронный документ отмечен у поставщика  
сертификационных услуг определенно  
числа и в определенное время;

9) подписывающее лицо – персона, у которой  
имеются средства создания электронной  
подписи и которая действует или от своего  
имени, или того физического или  
юридического лица, которого она  
представляет;

10) сертификационные услуги – выдача  
сертификатов, их аннулирование,  
приостановка и возобновление их действия,  
регистрация сертификатов, поддержка  
регистрационных проверочных данных  
электронных подписей, отметка электронных  
документов временной печатью, а также  
оказание консультационных услуг,  
связанных с электронной подписью;

11) сертификат – электронное подтверждение,  
которое связывает проверочные данные  
электронной подписи с подписывающим лицом  
и служит для идентификации подписывающего  
лица.

## 2 статья. Действие закона

(1) Этот закон определяет статус  
электронного документа и электронной  
подписи.

(2) Положения этого закона не применимы,  
если отметку электронного документа  
временной печатью осуществляет  
физическое или юридическое лицо, не  
являющееся поставщиком сертификационных  
услуг.

## Раздел II

### Электронный документ и его производные

### 3 статья. Электронный документ

(1) Требование, предъявляемое к документу в письменной форме, в отношении к электронному документу является исполненным, если у электронного документа имеется электронная подпись и электронный документ отвечает требованиям других нормативных актов.

(2) Электронный документ считается собственноручно подписанным, если у него есть безопасная электронная подпись. Электронный документ считается собственноручно подписанным также в тех случаях, когда у него имеется электронная подпись, и стороны письменно договорились о подписании электронного документа электронной подписью.

(3) В случаях, когда нормативные акты предусматривают, что документу в дополнение к остальным реквизитам требуется оттиск печати, это требование в отношении к электронному документу выполнено, если у электронного документа имеется безопасная электронная подпись и временная печать или электронная подпись, если стороны в порядке, оговоренном во второй части настоящей статьи, письменно договорились о подписании электронного документа электронной подписью.

(4) Электронная подпись является правовым доказательством, и не имеет ограничений для предоставления электронного документа как доказательства в компетентные органы, основываясь на том, что:

- 1) документ в электронной форме;
- 2) у него нет безопасной электронной печати.

(5) В электронном документообороте между государственными учреждениями и учреждениями самоуправления или между этими учреждениями и физическими лицами

электронный документ считается подписанным, если у него имеется безопасная электронная подпись и временная печать или электронная подпись, если стороны в порядке, оговоренном во второй части третьей статьи, письменно договорились о подписании электронного документа электронной подписью.

(6) Положения этого закона не распространяются на:

- 1) договоры, которыми создаются или передаются права на недвижимое имущество, за исключением права аренды;
- 2) договоры, которые в соответствии с законом не имеют силы, если они не подтверждены в порядке, предусмотренном законом;
- 3) договоры поручительства, если поручительство присваивают, и обеспечения залогов, если их предоставляет лицо, которое действует в целях, которые не связаны с ремеслом данного лица, предпринимательской деятельностью или профессией;
- 4) сделки в сфере семейного и наследственного права.

(С изменениями, которые сделаны законом от 28.10.2004, который вступает в силу 24.11.2004.)

#### **4 статья. Оригинал электронного документа**

(1) Если нормативные акты предписывают требование хранить или предъявлять оригинал документа, то это требование в отношении к электронному документу считается выполненным, если электронный документ отвечает требованиям второй и третьей частям третьей статьи настоящего закона.

(2) Первая часть этой статьи относится к обязанности в форме требования или случая, когда нормативные акты предусматривают юридические последствия за несохранение

или непредъявление оригинала документа.

## 5 статья. Производные электронного документа

(1) У копии электронного документа, заверенной копии или выписки в бумажной форме такая же юридическая сила, как и у оригинала, если достоверность копии, заверенной копии или выписки подтверждены в соответствии с требованиями нормативных актов, и, если предъявитель бумажной копии, заверенной копии или выписки по востребованию может предоставить оригинал документа в электронной форме, и он отвечает положениям этого закона.

(2) У электронной копии бумажного документа, заверенной копии или выписки такая же юридическая сила, как у оригинала, если лицо, у которого согласно с требованиями нормативных актов есть права заверять копии оригинальных документов, заверенных документов или выписок, подтвердил ее достоверность безопасной электронной подписью и временной печатью или электронной подписью, если стороны в порядке, оговоренном во второй части третьей статьи, письменно договорились о подписании электронного документа электронной подписью.

(3) Дубликата бумажного документа в электронной форме обладает такой же юридической силой, как у оригинала, если дубликат издан и оформлен в соответствии с положениями этого закона и требованиями других нормативных актов.

(4) Создавать производные электронных документов в бумажной форме возможно только от таких электронных документов, которые возможно предъявить в читаемом графическом виде.

(С изменениями, которые сделаны законом от 28.10.2004, который вступает в силу 24.11.2004.)

## Раздел III

# Правила оборота и хранения электронных документов

## 6 статья. Общие правила оборота и хранения электронных документов

(1) Если нормативные акты предусматривают для отдельных видов бумажных документов требования по их созданию, оформлению, хранению и обороту, то эти же требования относятся и к электронным документам.

(2) Правила создания, оформления, хранения и оборота для государственных учреждений и учреждений самоуправления и порядок, в котором происходит электронный документооборот между государственными учреждениями и учреждениями самоуправления или между этими учреждениями и физическими и юридическими лицами регламентируют правила кабинета Министров.

(3) Генеральная дирекция государственного архива ответственна за оценку и отбор электронных документов для долгосрочного и постоянного хранения, она же производит надзор, чтобы в архивах государственных учреждениях или учреждениях самоуправления были бы обеспечены сохранность и доступность электронных документов.

(4) Государственные учреждения и учреждения самоуправления разрабатывают инструкции внутреннего документооборота, которые отвечают требованиям этого закона и упомянутым во второй части этой статьи правилам кабинета Министров, а также специфике работы учреждения и обеспечивают физическим и юридическим лицам возможность подать документы, их копии, заверенные копии, выписки и дубликаты в государственные учреждения и учреждения самоуправления и получить от

них ответ в электронной или другой форме по желанию этого лица.

(5) Способ оценки электронного документа, порядок и срок хранения, по которым они должны сдаваться в государственный архив для хранения, регламентируют правила кабинета Министров.

(С изменениями, которые сделаны законом от 06.05.2004, который вступает в силу 27.05.2004.)

## 7 статья. Специфические условия хранения электронных документов

(1) Если нормативные акты предусматривают, что определенные документы, записи или данные необходимо сохранять, то это же требование в отношении к электронному документу является выполненным в случае, если:

5) данные, которые он включает, доступны для использования;

6) электронный документ сохранен в такой же форме, в которой он изначально создан, отослан или принят, или в такой форме, в которой видны изначально созданные, отосланные или полученные данные;

7) сохраненные данные позволяют определить происхождение электронного документа или пункт назначения, время отсылки или приема.

(2) условия третьего пункта первой части этой статьи не распространяются на данные, которые созданы автоматически в процессе их приема или отправки.

(3) Лицо может выполнить условия первой части этой статьи, используя услуги другого лица, если соблюдены положения этого закона.

## Раздел IV

### Поставщик сертификационных услуг и доверительный поставщик сертификационных



## 8 статья. Поставщик сертификационных услуг

(1) Поставщиком сертификационных услуг является физическое или юридическое лицо, которое предоставляет сертификационные услуги без специального разрешения.

(2) Аккредитация поставщика сертификационных услуг является добровольной.

(3) Поставщик сертификационных услуг считается доверительным, если он отвечает требованиям девятой статьи этого закона.

## 9 статья. Доверительный поставщик сертификационных услуг

Доверительным поставщиком сертификационных услуг считается физическое или юридическое лицо, которое отвечает следующим требованиям:

1) использует надежный персонал, который обладает специфическими знаниями по предоставлению сертификационных услуг, опытом, квалификацией, который ознакомлен с соответствующими правилами безопасности оказания сертификационных услуг и не был осужден за умышленное преступное деяние;

2) использует надежные и безопасные информационную систему и продукты, которые достаточно защищены от несанкционированного доступа и модификаций;

3) содержит достаточные финансовые ресурсы для того, чтобы выполнить условия этого закона и выпущенных нормативных актов и в определенном объеме и порядке застраховал свою гражданско-правовую ответственность своей профессиональной деятельностью в соответствии с четырнадцатой статьей

этого закона;

- 4) аккредитовано в государственной инспекции данных (далее в тексте также – учреждение надзора) в предусмотренном в этом законе порядке;
- 5) обеспечивает бесперебойный доступ к регистру проверки электронных подписей в режиме непосредственного доступа.
- 6) обеспечивает незамедлительное аннулирование квалификационного сертификата, возможность приостановить или возобновить его действие в случаях, предусмотренных в этом законе;
- 7) обеспечивает, чтобы в любой момент можно было бы констатировать число и время выдачи, аннулирования, приостановки и возобновления квалификационного сертификата;
- 8) использует безопасную систему хранения квалификационных сертификатов в доступной для проверки форме и обеспечивает, чтобы:
  - а) только надежный полномочный представитель поставщика сертификационных услуг мог сделать записи или изменения в них,
  - б) было возможно проверить и констатировать изменения в информации;
  - с) выданные квалификационные сертификаты недоступны публично, за исключением случаев, когда получено письменное на то разрешение подписывающего лица,
  - д) любые технические изменения, которые касаются требований безопасности, видны системному администратору,
  - е) была использована такая технология, чтобы, используя данные для создания электронной подписи, они никогда не могли бы быть копированы;
- 9) отмечая электронный документ временной печатью, обеспечивает возможность установить неоспоримое число и время полученного электронного документа;
- 10) обеспечивает, чтобы временная печать не

и изменяла подписываемый электронный документ.

(С изменениями, которые сделаны законом от 28.10.2004, который вступает в силу 24.11.2004.)

## 10 статья. Аккредитация доверительного поставщика сертификационных услуг

Для того чтобы получить аккредитацию, учреждению надзора предоставляются следующие документы:

- 1) письменное заявление;
- 2) правила предоставления сертификационных услуг;
- 3) описание безопасности и процедур предоставления сертификационных услуг;
- 4) заключения о проверке безопасности информационной системы и процедур по предоставлению сертификационных услуг;
- 5) документ, который подтверждает, что требования третьего пункта девятой статьи этого закона выполнены.

## 11 статья. Правила предоставления сертификационных услуг

(1) В правила предоставления сертификационных услуг включены:

- 1) фирма, регистрационный номер или фамилия, имя, персональный код, адрес, телефон и адрес электронной почты доверительного поставщика сертификационных услуг;
- 2) информация об используемых для предоставления сертификационных услугах системах, аппаратуре, технологиях, программном обеспечении и документах о правах на его использование;
- 3) образец договора между доверительным поставщиком сертификационных услуг и подписывающего лица;
- 4) информация о процедуре и безопасности

- выдачи квалификационного сертификата;
- 5) информация о различных возможностях подписывающего лица ограничить применение безопасной электронной подписи;
- 6) информация о процедурах аннулирования квалификационного сертификата, приостановке его действия и возобновления;
- 7) информация о технических и технологических возможностях, которые предлагает поставщик сертификатов, чтобы защитить средства создания безопасной электронной подписи, проверочные данные электронной подписи и квалификационный сертификат от незаконного использования;
- 8) информация о том, как обеспечен свободный доступ к регистрам проверочных данных электронных подписей, выданных, аннулированных, приостановленных и возобновленных сертификатов в режиме непосредственного доступа;
- 9) информация об отметке документа временной печатью и безопасности этой процедуры;
- 10) информация о том, как в режиме непосредственного доступа обеспечен доступ к регистру временных печатей;
- (2) Если меняется информация, включенная в правила поставщика сертификатов, доверительный поставщик услуг незамедлительно предоставляет учреждению надзора изменения в правилах поставщика сертификатов.

## 12 статья. Описание безопасности информационной системы поставщика сертификатов, аппаратуры и процедур

- (1) Указываемую в описании информацию о безопасности информационной системы поставщика сертификатов,

аппаратуре и процедурах определяет кабинет Министров.

(2) Если меняются информация в описании безопасности системы поставщика сертификационных услуг, аппаратуре и процедурах, доверительный поставщик сертификационных услуг незамедлительно предоставляет учреждению надзора изменения в описании безопасности информационной системы, аппаратуры и процедур.

### 13 статья. Проверка безопасности информационной системы поставщика сертификационных услуг, аппаратуры и процедур

(1) Безопасности информационной системы поставщика сертификационных услуг, аппаратуры и процедур проверяет и дает об этом заключение эксперт, который включен в утвержденный список учреждения надзора.

(2) В утвержденный список учреждения надзора включают лицо, которое отвечает всем следующим требованиям:

- 1) у него имеется технические возможности определить соответствие безопасности информационной системы поставщика сертификационных услуг, аппаратуры и процедур требованиям нормативных актов;
- 2) оно юридически и финансово независимо от доверительных поставщиков сертификационных услуг и учреждений надзора;
- 3) у него или у его рабочего персонала имеются необходимые знания;
- 4) оно не занимается системой предоставления сертификационных услуг и производством и поставками других информационных технологий.

(3) Порядок и сроки проверки безопасности информационной системы поставщика сертификационных услуг, аппаратуры и процедур определяет кабинет Министров.

14 статья. Страхование гражданско-правовой ответственности

(1) Риск, связанный с возможным ущербом от деятельности доверительного поставщика сертификационных услуг, должен быть обязательно застрахован.

(2) Страхование рисков деятельности доверительного поставщика сертификационных услуг обеспечивает задолженности, которые могут возникнуть в результате его деятельности.

(3) Договор страхования доверительного поставщика сертификационных услуг необходимо заключить до получения аккредитации, и договор страхования необходимо поддерживать в силе на протяжении всего времени предоставления сертификационных услуг.

(4) Если в результате деятельности или бездействия доверительного поставщика сертификационных услуг возник ущерб, страховое общество, основываясь на договоре страхования, покрывает этот ущерб из страховой премии доверительного поставщика сертификационных услуг.

(5) Минимальную страховую сумму определяет кабинет Министров.

(С изменениями, которые сделаны законом от 28.10.2004, который вступает в силу 24.11.2004.)

#### 141 статья. Технические и организаторские требования

Кабинет Министров определяет технические и организаторские требования, которым отвечает квалификационный сертификат, доверительный поставщик сертификационных услуг, средства создания безопасной электронной подписи, а также порядок, в котором должна происходить безопасная верификация электронной подписи.

(Редакция закона от 28.10.2004, которая вступает в силу 24.11.2004)

## 15 статья. Защита данных физических лиц

(1) Данные физических лиц поставщик сертификационных услуг может получить только непосредственно от подписывающего лица или от третьего лица, если подписывающее лицо с этим согласилось.

(2) Поставщик сертификационных услуг может обрабатывать данные физических лиц только с целью выдать и содержать сертификат.

(3) Поставщику сертификационных услуг без согласия подписывающего лица нельзя обрабатывать данные для других целей.

### Раздел V

## Квалификационный сертификат

## 16 статья. Информация, входящая в квалификационный сертификат

(1) Квалификационный сертификат содержит следующую информацию:

- 1) ссылку, что это квалификационный сертификат;
- 2) фирму доверительного поставщика сертификационных услуг, регистрационный номер, страну учреждения или имя, фамилию и персональный код;
- 3) имя и фамилию подписывающего лица или псевдоним, указав, что это псевдоним;
- 4) персональный код подписывающего лица;
- 5) срок действия квалификационного сертификата;
- 6) присвоенный доверительным поставщиком сертификационных услуг порядковый номер сертификата;
- 7) проверочные данные электронной подписи, которые соответствуют подконтрольным подписывающему лицу данным для создания электронной подписи.

(2) Дополнительно к информации, упомянутой в первой части этой статьи, квалификационный сертификат может

содержать следующую информацию:

- 1) сферу деятельности квалификационного сертификата иди других ограничений действия сертификата;
- 2) относящийся к подписывающему лицу специфический юридический факт (если это нужно) в зависимости от целей, для которых предназначен квалификационный сертификат;
- 3) ограничение суммы сделок, для которых можно использовать квалификационный сертификат;
- 4) идентификационный номер подписывающего лица.

(3) Кв а л и ф и к а ц и о н н ы й с е р т и ф и к а т подписывает доверительный поставщик сертификационных услуг электронной подписью. Электронная подпись отвечает следующим требованиям:

- 1) она привязана только к доверительному поставщику сертификационных услуг;
- 2) она обеспечивает идентификацию доверительного поставщика сертификационных услуг;
- 3) она создана с помощью средств создания электронной подписи, которые принадлежат доверительному поставщику сертификационных услуг;
- 4) она связана с подписанным электронным документом таким образом, что последующие изменения подписанного электронного документа стали бы заметны.

(С изменениями, сделанными законом от 22.06.2006, которые вступают в силу 21.07.2006)

## 17 статья. Выдача квалификационного сертификата

(1) Чт о б ы п о л у ч и т ь к в а л и ф и к а ц и о н н ы й сертификат, подписывающим лицом подается письменное заявление.

(2) П е р е д в ы д а ч е й к в а л и ф и к а ц и о н н о г о сертификата доверительный поставщик сертификационных услуг в присутствии подписывающего лица удостоверяется в



идентичности подписывающего лица, основываясь на документе, удостоверяющего личность.

(3) После письменного требования подписывающего лица доверительный поставщик сертификационных услуг включает информацию о полномочиях или другую значимую информацию, которая упомянута во второй части шестнадцатой статьи.

(4) После письменного требования подписывающего лица доверительный поставщик сертификационных услуг вместо имени и фамилии может вписать псевдоним, сделав об этом соответствующую отметку в сертификате.

(5) Квалификационный сертификат подписывающему лицу выдает доверительный поставщик сертификационных услуг.

(6) Подписывающему лицу можно выдать несколько квалификационных сертификатов.

(7) Доверительный поставщик сертификационных услуг, сохраняя оговоренную в этом законе ответственность, на договорной основе может доверить деятельность, упомянутую во втором, третьем и четвертом разделах этой статьи, другому лицу, если на это письменно согласится учреждение надзора.

## 18 статья. Аннулирование квалификационного сертификата, приостановка и возобновление его действия

(1) Аннулирование квалификационного сертификата это признание его недействительным. Действие аннулированного сертификата нельзя восстановить.

(2) Доверительный поставщик сертификационных услуг незамедлительно аннулирует квалификационный сертификат в следующих случаях:

- 1) подписывающее лицо потребовало аннулировать сертификат;
  - 2) доверительный поставщик сертификационных услуг получил официальную информацию о смерти подписывающего лица или изменяется другая, включенная в сертификат, информация;
  - 3) подписывающее лицо сообщил доверительному поставщику сертификационных услуг неправильные или могущие ввести в заблуждение данные, чтобы получить квалификационный сертификат;
  - 4) выполняя решение суда об аннулировании квалификационного сертификата;
  - 5) в определенных в договоре о сертификационных услугах случаях.
- (3) Приостановка действия квалификационного сертификата – это временное признание его недействительным. Действие приостановленного сертификата можно возобновить.
- (4) Возобновление квалификационного сертификата – это признание действительным такого квалификационного сертификата, действие которого было приостановлено.
- (5) Доверительный поставщик сертификационных услуг приостанавливает и возобновляет действия квалификационного сертификата в следующих случаях:
- 1) исполняя решение суда;
  - 2) основываясь на письменном требовании подписывающего лица;
  - 3) в случаях, предусмотренных в договоре об оказании сертификационных услуг;
- (6) Квалификационный сертификат нельзя аннулировать и приостановить или возобновить его действие обратным числом.
- (7) Безопасная электронная подпись недействительна с момента аннулирования и приостановки квалификационного сертификата.
- (8) В случае смерти подписывающего лица,

электронная подпись недействительна с момента смерти подписывающего лица.

(9) В случае, когда доверительный поставщик сертификационных услуг без правовых оснований, со злым умыслом или по неосторожности аннулирует квалификационный сертификат, приостановит или возобновит его действие, доверительный поставщик сертификационных услуг возмещает лицам убытки, которые возникли в результате необоснованного аннулирования квалификационного сертификата, приостановки или возобновления его действия.  
(С изменениями, сделанными законом от 22.06.2006, которые вступают в силу 21.07.2006)

## Раздел VI

### Надзор за доверительным поставщиком сертификационных услуг

#### 19 статья. Учреждение надзора за доверительным поставщиком сертификационных услуг

(1) Надзирающим за доверительным поставщиком сертификационных услуг учреждением является государственная инспекция данных.

(2) Учреждение надзора регулярно следит за соответствием деятельности доверительного поставщика сертификационных услуг требованиям этого закона и других нормативных актов.

#### 20 статья. Обязанности учреждения надзора

(1) Учреждения надзора имеют следующие обязанности:

1) аккредитовать поставщиков сертификационных услуг согласно добровольному принципу аккредитации;

- 2) проверять, соблюдают ли доверительные поставщики сертификационных услуг правила оказания сертификационных услуг;
- 3) следить за тем, чтобы безопасность информационной системы и процедур доверительного поставщика сертификационных услуг соответствует требованиям этого закона, других нормативных актов и описанию безопасности информационной системы предоставления сертификационных услуг, аппаратуры и процедур;
- 4) следить за тем, чтобы доверительного поставщика сертификационных услуг регистры выданных, аннулированных, приостановленных и возобновленных проверочных данных электронных подписей квалификационных сертификатов были бы доступны в режиме непосредственного доступа;
- 5) обеспечить, чтобы регистр аккредитованного в Латвии доверительного поставщика сертификационных услуг, в который также должна включаться информация о поставщиках сертификационных услуг других стран, выданные квалификационные сертификаты которых гарантирует аккредитованный в Латвии доверительный поставщик сертификационных услуг, был бы свободно доступен в режиме непосредственного доступа.

(2) Учреждение надзора содержит в режиме непосредственного доступа свободно доступный регистр доверительных поставщиков сертификационных услуг, в котором доступна следующая информация:

- 1) фирма или имя и фамилия доверительного поставщика сертификационных услуг;
- 2) адрес, телефон, адрес электронной почты доверительного поставщика сертификационных услуг;
- 3) правила предоставления сертификационных услуг;

- 4) описание безопасности информационной системы, аппаратуры и процедур поставщика сертификационных услуг;
  - 5) заключения о безопасности информационной системы, аппаратуры и процедур поставщика сертификационных услуг;
  - 6) дата аккредитации;
  - 7) информация о замечаниях, предупреждениях учреждения надзора или аннулировании аккредитации.
- (3) Если внесенные поставщиком сертификационных услуг документы отвечают требованиям этого закона и других нормативных актов, то учреждение надзора в течение 10 дней со дня внесения документов, указанных в десятой статье этого закона, выдает поставщику сертификационных услуг аккредитационное удостоверение и включает информацию, упомянутую во второй части этой статьи, в регистр доверительных поставщиков сертификационных услуг.
- (4) Если внесенные документы или поставщик сертификационных услуг не отвечает требованиям этого закона и нормативных актов, то учреждение надзора в десятидневный срок со дня получения упомянутых в десятой статье этого закона документов выдает поставщику сертификационных услуг отказ в письменном виде.

## 21 статья. Мероприятия надзора

- (1) У учреждения надзора есть права давать указания доверительному поставщику сертификационных услуг, чтобы устранить несоответствия этому закону, другим нормативным актам, включенным в регистр правилам оказания сертификационных услуг доверительного поставщика сертификационных услуг или описанию безопасности системы оказания

сертификационных услуг, аппаратуры и процедур.

(2) Срок устранения несоответствий определяет учреждение надзора.

(3) Если указания учреждения надзора не выполнены в указанный срок, учреждение надзора предупреждает доверительного поставщика сертификационных услуг о возможном аннулировании аккредитации.

(4) Если в течение десяти дней после предупреждения об аннулировании аккредитации, вынесенного учреждением надзора, указания учреждения надзора не выполнены, аккредитация доверительного поставщика сертификационных услуг подлежит незамедлительному аннулированию и информация об аннулировании аккредитации подлежит включению в регистр доверительных поставщиков сертификационных услуг.

(5) После аннулирования аккредитации доверительного поставщика сертификационных услуг применимы правила, оговоренные во второй, третьей, четвертой и пятой частях двадцать второй статьи этого закона.

(6) Проводя надзор, должностное лицо учреждения надзора предъявляет служебное удостоверение. У упомянутого лица есть следующие права:

1) свободно посещать любые нежилые помещения, в которых находится информационная система и аппаратура доверительного поставщика сертификационных услуг, и в присутствии доверительного поставщика сертификационных услуг вести необходимую проверку или другие мероприятия, чтобы определить соответствие процесса предоставления сертификационных услуг этому закону, другим нормативным актам, внесленным в регистр доверительного поставщика сертификационных услуг правилам оказания сертификационных услуг

и описанию безопасности системы оказания сертифицированных услуг, аппаратуры и процедур;

2) потребовать от представителей и работников доверительного поставщика сертифицированных услуг письменное или устное объяснение;

3) ознакомиться с документами и другой информацией, относящейся к предоставлению сертифицированных услуг;

4) потребовать проверку информационной системы предоставления сертифицированных услуг, аппаратуры и процедур и назначить независимую экспертизу для исследования проверяемого вопроса.

(7) Учреждения надзора есть право обратиться в суд с иском о прекращении деятельности доверительного поставщика сертифицированных услуг, если соответствующий доверительный поставщик сертифицированных услуг нарушил этот закон или другие нормативные акты.

(8) Решения учреждения надзора можно обжаловать в суде.

## 22 статья. Прекращение деятельности доверительного поставщика сертифицированных услуг, объявление о неплатежеспособности и приостановка оказания сертифицированных услуг

(1) Доверительный поставщик сертифицированных услуг незамедлительно письменно информирует учреждение надзора и подписывающих лиц, с которыми заключен договор о предоставлении сертифицированных услуг, что их работа прекращена, что он объявлен неплатежеспособным или что предоставление сертифицированных услуг приостановлена.

(2) В упомянутой в первой части этой статьи случаях доверительный поставщик сертифицированных услуг обеспечивает

сохранность связанной с сертификационными услугами данных, информации, базы данных, регистра, другой принадлежащей информации, информационную систему и сертификационные услуги и после обоюдного согласия передает все это другому доверительному поставщику сертификационных услуг.

(3) Обо всех процедурах передачи и сроках незамедлительно письменно информируется учреждение надзора.

(4) Если упомянутая во второй части этой статьи передача невозможна, то доверительный поставщик сертификационных услуг под надзором учреждения надзора передает данные, связанные с сертификационными услугами, информацию, базы данных, регистр, другую принадлежащую информацию, информационную систему и сертификационные услуги в государственный архив.

(5) Подписывающее лицо после того, как получил информацию о прекращении деятельности доверительного поставщика сертификационных услуг, объявлении о неплатежеспособности или приостановке предоставления услуг, вправе передать свои связанные с выданным квалификационным сертификатом данные другому доверительному поставщику сертификационных услуг по своему усмотрению.

(6) Учреждение надзора незамедлительно аннулирует аккредитацию прекратившей деятельность, объявленного неплатежеспособным или приостановленным в предоставлении сертификационных услуг доверительного поставщика сертификационных услуг, включая информацию об этом в регистр доверительных поставщиков сертификационных услуг.

## Раздел VII



## Права и обязанности доверительного поставщика сертификационных услуг и подписывающего лица

### 23 статья. Обязанности доверительного поставщика сертификационных услуг

У доверительного поставщика сертификационных услуг есть следующие обязанности:

- 1) использовать безопасную систему предоставления сертификационных услуг, аппаратуру и процедуры, которые гарантируют достаточную безопасность сертификационных услуг;
- 2) производить необходимые мероприятия, чтобы гарантировать секретность данных для создания электронной подписи и защиту от незаконной обработки и использования данных для создания электронной подписи, защиту квалификационных сертификатов от подделки и доступность к этому сертификату только с согласия подписываемого лица;
- 3) обеспечить информационную систему предоставления сертификационных услуг, аппаратуру и процедуры в соответствии с этим законом и другим нормативным актам;
- 4) обеспечить, чтобы в квалификационный сертификат включили идентификационную информацию подписывающего лица, основываясь только на предъявленный в присутствии подписывающего лица документ, удостоверяющий его личность;
- 5) обеспечить, чтобы выдали квалификационный сертификат, заключив с подписывающим лицом договор о предоставлении сертификационных услуг;
- 6) перед заключением договора письменно информировать подписывающее лицо о правилах и условиях, которые относятся к использованию квалификационного

сертификата, в том числе о любых ограничениях использования сертификата, о процедурах рассмотрения жалоб и споров, о гражданско-правовой ответственности доверительного поставщика сертификационных услуг, а также о предусмотренных в договоре случаях аннулирования, приостановления и возобновления действия квалификационного сертификата. Информацию можно отослать в электронном виде, заверив ее безопасной электронной подписью доверительного поставщика сертификационных услуг.

Соответствующие части этой информации делают доступными лицам, которые доверяют квалификационному сертификату, по требованию этих лиц;

7) перед заключением договора письменно информировать подписывающее лицо о правилах оказания сертификационных услуг и мер безопасности, которые проводит доверительный поставщик сертификационных услуг, чтобы предотвратить незаконное использование выданного квалификационного сертификата;

8) после выдачи квалификационного сертификата письменно информировать подписывающее лицо о включенных в сертификат условиях и ограничениях использования сертификата;

9) соблюдать этот закон, другие нормативные акты, включенные в регистр доверительных поставщиков сертификационных услуг правила предоставления сертификационных услуг и описание безопасности информационно-системы предоставления сертификационных услуг и процедур;

10) незамедлительно информировать учреждение надзора обо всех обстоятельствах, которые задерживают исполнять этот закон, другие нормативные акты, включенные в регистр доверительных поставщиков сертификационных услуг правил предоставления сертификационных услуг или описание безопасности

- информационной системы предоставления  
сертификационных услуг и процедур;
- 11) в случаях, упомянутых во второй части  
восемнадцатой статьи, незамедлительно  
аннулировать квалификационный  
сертификат;
- 12) если нельзя незамедлительно и уверенно  
подтвердить факты, упомянутые в пунктах 2 и  
3 второй части восемнадцатой статьи этого  
закона, то приостановить действие  
квалификационного сертификата до  
выяснения соответствующих фактов;
- 13) незамедлительно информировать  
подписывающее лицо, его доверенное лицо  
или наследников об аннулировании или  
приостановлении действия  
квалификационного сертификата;
- 14) постоянно поддерживать бесплатные  
свободно доступные регистры полные  
проверочные данные электронной подписи,  
выданных, аннулированных,  
приостановленных и возобновленных  
квалификационных сертификатов;
- 15) вести полный учет выдачи, аннулирования  
квалификационных сертификатов,  
приостановления и возобновления их  
деятельности, а также учет процедур  
временных печатей;
- 16) сохранять в течение определенного  
времени и в порядке, предусмотренном этим  
законом и другими нормативными актами,  
информацию, связанную с временной печатью  
и квалифицированным сертификатом;
- 17) регулярно проводить проверки связанной  
с сертификационными услугами  
информационной системы, аппаратуры и  
процедуры и хранить данные проверок. В  
записях о проверках необходимо  
фиксировать все мероприятия, которые  
связаны с выдачей квалификационных  
сертификатов, аннулированием,  
приостановкой и возобновлением их  
деятельности, мероприятия, которые  
связаны с отметкой документов временной

- печатью, а также любые другие изменения данных. Данные проверок хранятся постоянно. Данным проверок обеспечена нормативными актами определенная физическая и логическая защита;
- 18) проводить мероприятия по обеспечению безопасности против возможных подделок квалификационных сертификатов и временных печатей, гарантировать конфиденциальность данных для создания электронной подписи во время ее создания;
- 19) не хранить и не копировать данные для создания электронной подписи;
- 20) обеспечить, чтобы временная печать указывало на международно-скоординированное точное время;
- 21) в порядке, определенным в нормативных актах, предоставлять судам, прокуратуре и справочным службам информацию об аннулированных, приостановленных и возобновленных сертификатах и временных печатях;
- 22) соблюдать закон о защите данных физических лиц и нормативные акты, которые регулируют безопасность информационной системы;
- 23) передать регистр аннулированных и прекративших свое действие сертификатов государственному архиву согласно с соответствующими правилами кабинета Министров, которые регламентируют порядок и сроки, в которых электронные документы оцениваются, накапливаются и передаются в государственный архив;
- 24) застраховать свою гражданско-правовую ответственность.  
(С изменениями, сделанными законом от 22.06.2006, который вступает в силу 21.07.2006.)

## **24 статья. Ответственность доверительного поставщика сертификационных услуг**

- (1) Доверительный поставщик сертификационных услуг ответственен за

убытки, причиненные лицу, которое сознательно положилось на квалификационный сертификат в отношении:

- 1) соблюдения требований этого закона и нормативных актов, выдав квалификационный сертификат, а также к соблюдению и исполнению включенного в регистр доверительных поставщиков сертификационных услуг правила предоставления сертификационных услуг или описания безопасности информационной системы оказания сертификационных услуг, аппаратуры и процедур;
- 2) включенной в квалификационный сертификат информации;
- 3) соответствия данных для создания электронной подписи проверочным данным электронной подписи в момент выдачи квалификационного сертификата;
- 4) использования данных для создания электронной подписи и проверочных данных электронной подписи в благоразумном виде;

(2) Доверительный поставщик сертификационных услуг ответственен за убытки, причиненные лицу, которое сознательно положилось на квалификационный сертификат, когда не зарегистрировано аннулирование этого сертификата или приостановка его действия;

(3) Доверительный поставщик сертификационных услуг не несет ответственности за убытки, причиненные лицу, которое сознательно положилось на квалификационный сертификат, который был использован, не соблюдая включенных в него условий или ограничений или превысив указанную в сертификате сумму сделки.

## 25 статья. Права и обязанности подписывающего лица

(1) У подписывающего лица имеются следующие

обязанности:

- 1) предоставить доверительному поставщику сертификационных услуг достоверную информацию;
  - 2) до того, как заключен договор об оказании сертификационных услуг, письменно подтвердить, что ознакомился с включенными в регистр доверительных поставщиков сертификационных услуг правилами оказания сертификационных услуг, описанием безопасности информационной системы оказания сертификационных услуг, аппаратуры и процедур и других мероприятий безопасности, которые проводит доверительный поставщик сертификационных услуг, чтобы предотвратить незаконное использование квалификационного сертификата;
  - 3) после получения квалификационного сертификата письменно подтвердить, что ознакомился с включенными в квалификационной сертификат условиями и ограничениями;
  - 4) обеспечить, чтобы данные для создания электронной подписи не могли бы быть использованы без ведома подписывающего лица;
  - 5) незамедлительно потребовать, чтобы доверительный поставщик сертификационных услуг аннулировал квалификационный сертификат или приостановил его действие, если есть основание считать, что данные для создания электронной подписи были использованы без ведома подписывающего лица;
  - 6) незамедлительно потребовать, чтобы доверительный поставщик сертификационных услуг аннулировал квалификационный сертификат, если меняется включенная в него информация;
- (2) Подписывающее лицо ответственно за убытки, которые причинены лицу, которое сознательно положилось на квалификационный сертификат, если:
- 1) подписывающее лицо предоставляет

доверительному поставщику  
сертификационных услуг недостоверную  
информацию;

- 2) подписывающее лицо достаточно не  
заботится о защите против  
несанкционированного использования  
данных для создания электронной подписи;
- 3) было основание считать, что данные для  
создания электронной подписи  
использованы без ведома подписывающего  
лица, но подписывающее лицо не  
потребовало, чтобы доверительный  
поставщик сертификационных услуг  
аннулировал квалификационный сертификат  
или приостановил его действие.

## Раздел VIII

### Признание зарубежных квалификационных сертификатов

#### 26 статья. Признание зарубежных квалификационных сертификатов

У выданных за рубежом квалификационных  
сертификатов имеется определенный в этом  
законе юридический статус и правовые  
последствия, если статус сертификата и  
связанные с сертификатом проверочные  
данные можно проверить, находясь в Латвии,  
и квалификационный сертификат отвечает  
как минимум одному из следующих условий:

- 1) он отвечает всем требованиям этого  
закона и нормативных актов;
- 2) его выдал добровольно аккредитованный в  
учреждении надзора поставщик  
сертификационных услуг;
- 3) его гарантирует добровольно  
аккредитованный в учреждении надзора  
поставщик сертификационных услуг;
- 4) его признает Латвийская Республика  
согласно международным договорам;

5) он выдан зарегистрированный в стране-участнице Европейского Союза поставщик сертификационных услуг или его гарантирует зарегистрированный в стране-участнице Европейского Союза поставщик сертификационных услуг.

(С изменениями, сделанными законом от 28.10.2004, которые вступают в силу 24.11.2004.)

## Другие правила

1. У государственных учреждений и учреждений самоуправления имеется обязанность принимать электронные документы от физических и юридических лиц не позднее, чем 1 января 2004 года.

2. До 1 января 2005 года кабинет Министров издает оговоренные в статье 141 правила. (Редакция, которая сделана законом от 28.10.2004, который вступает в силу 24.11.2004.)

## Информативная ссылка на директиву Европейского Союза

(Редакция закона от 22.06.2006, которая вступает в силу 21.07.2006.)

В закон включены правовые нормы, которые исходят из директивы Европейского Парламента и Совета 1999/93/ЕК от 13 декабря 1999 года о систему электронной подписи Европейского сообщества.

Закон вступает в силу 1 января 2003 года.

Закон принят Саэймом 31 октября 2002 года.

Вместо президента Государства  
Председатель саэйма И. Удре  
Рига, 20 ноября 2002 года