



**Постановление об утверждении Положения о порядке
применения цифровой подписи в электронных документах
органов публичной власти**

№ 320 от 28.03.2006

Мониторул Официал ал Р.Молдова № 51-54/350 от 31.03.2006

* * *

Во исполнение части (3) статьи 18 Закона об электронном документе и цифровой подписи № 264-XV от 15 июля 2004 г. (Официальный монитор Республики Молдова, 2004 г., № 132-137, ст.710) Правительство

ПОСТАНОВЛЯЕТ:

1. Утвердить Положение о порядке применения цифровой подписи в электронных документах органов публичной власти (прилагается).
2. Поручить органам центрального публичного управления и рекомендовать органам местного публичного управления создать в 3-месячный срок необходимые условия для применения цифровой подписи в соответствии с утвержденным Положением.
3. Академии публичного управления при Президенте Республики Молдова совместно с государственным предприятием "Centrul de telecomunicații speciale" Службы информации и безопасности организовать курсы обучения служащих органов публичной власти по применению цифровой подписи.
4. Услуги по сертификации открытых ключей и иные виды услуг, связанные с цифровой подписью, предоставляются в соответствии с главой III Положения о специальных телекоммуникационных системах Республики Молдова, утвержденного Постановлением Правительства № 735 от 11 июня 2002 г. (Официальный монитор Республики Молдова, 2002 г., № 79-81, ст.833) (с последующими изменениями и дополнениями).

ПРЕМЬЕР-МИНИСТР
Контрассигнует:
министр информационного
развития

Василе ТАРЛЕВ

Владимир Моложен

Кишинэу, 28 марта 2006 г.
№ 320.

Утверждено
Постановлением Правительства
№ 320 от 28 марта 2006 г.

ПОЛОЖЕНИЕ

о порядке применения цифровой подписи в
электронных документах органов публичной власти

I. Общие положения

1. Настоящее Положение разработано на основании Закона об электронном документе и цифровой подписи № 264-XV от 15 июля 2004 г. и определяет общие условия применения цифровой подписи в электронных документах органов публичной власти.
2. Орган публичной власти на договорных условиях получает услуги по сертификации открытых ключей и иные виды услуг, связанных с цифровой подписью, от центра сертификации открытых ключей органов публичного управления (в дальнейшем - центр сертификации) в соответствии с его регламентом и осуществляет обмен информацией с центром сертификации через телекоммуникационную систему органов публичного управления.
3. Орган публичной власти применяет цифровую подпись только при

условии использования средств цифровой подписи, имеющих сертификат соответствия, выданный согласно действующему законодательству. До создания органов по оценке соответствия средств цифровой подписи могут использоваться средства цифровой подписи, имеющие положительное заключение от уполномоченного органа по разработке и реализации государственной политики и контролю в сфере применения цифровой подписи (в дальнейшем – уполномоченный орган).

4. Служащие органа публичной власти применяют цифровую подпись в электронных платежных документах или при совершении сделок в пределах сумм, указанных в сертификатах открытых ключей.

5. Ответственность за организацию применения цифровой подписи в электронных документах органа публичной власти несет его руководитель.

II. Порядок применения цифровой подписи

6. Применение цифровой подписи предусматривает:

- a) создание открытого и закрытого ключей;
- b) сертификацию открытого ключа в центре сертификации;
- c) подписание электронного документа цифровой подписью;
- d) проверку подлинности цифровой подписи в электронном документе.

7. Цифровая подпись в электронных документах органов публичной власти применяется лицом, уполномоченным в установленном порядке подписывать собственноручной подписью подобные документы на бумажном носителе (в дальнейшем – служащий).

8. Внутренний порядок применения цифровой подписи в электронных документах органа публичной власти, который предусматривает, в частности, порядок создания, согласования и подписания электронных документов, проверки подлинности цифровой подписи, правила ведения учета, хранения и уничтожения закрытых ключей, порядок предоставления центру сертификации информации, необходимой для создания, приостановления и возобновления действия, отзыва сертификатов открытых ключей утверждается руководителем органа публичной власти в соответствии с установленными требованиями в сфере цифровой подписи.

9. Подразделение информационных технологий органа публичной власти, а при отсутствии такового – подразделение или сотрудник, назначенные приказом руководителя данного органа (далее – ответственное подразделение):

a) консультирует служащих в процессе создания закрытых и открытых ключей, а также при подписании электронных документов и проверке подлинности цифровой подписи;

b) подготавливает и предоставляет центру сертификации информацию, необходимую для создания сертификатов открытых ключей служащих, а также обращения о приостановлении и возобновлении действия и об отзыве сертификатов;

c) обеспечивает доступ служащих к реестрам сертификатов открытых ключей, которые ведутся центрами сертификации открытых ключей;

d) ведет учет средств цифровой подписи, используемых в органе публичной власти;

e) ведет учет материальных носителей закрытых ключей служащих;

f) обеспечивает хранение документов, на основании которых были созданы сертификаты открытых ключей служащих;

g) осуществляет внутренний контроль за использованием служащими средств цифровой подписи и за хранением материальных носителей закрытых ключей в соответствии с установленными требованиями.

Раздел 1. Создание закрытого и открытого ключей

10. Создание закрытого и открытого ключей производится служащим лично и непосредственно в органе публичной власти или в центре сертификации. В случае необходимости в процессе создания закрытого и открытого ключей служащему предоставляется помощь ответственным подразделением или персоналом центра сертификации без нарушения конфиденциальности закрытого ключа.

Раздел 2. Сертификация открытого ключа в центре сертификации

11. Служащий может подписывать электронные документы после получения сертификата открытого ключа в центре сертификации.

12. Руководитель органа публичной власти либо иное лицо, назначенное руководителем, направляет центру сертификации список служащих, открытые ключи которых необходимо сертифицировать, с указанием фамилий и имен данных лиц, занимаемых должностей, данных об ответственном подразделении, а также при необходимости предельной суммы, для которой действительно применение цифровой подписи в электронных платежных документах или при совершении сделок (в молдавских леях).

13. На основании списка, указанного в пункте 12 настоящего Положения, центр сертификации принимает заявки на сертификацию открытых ключей в электронной форме на материальном носителе или по защищенному каналу связи в соответствии с требованиями уполномоченного органа.

14. Заявка на сертификацию открытого ключа, составляемая служащим, должна содержать:

a) наименование органа публичной власти и его идентификационный код IDNO;

b) фамилию и имя служащего, номер документа, удостоверяющего личность, и идентификационный номер физического лица IDNP, занимаемую им должность;

c) информацию, необходимую для передачи сообщений служащему (номера телефонов, факса, адрес электронной почты);

d) сертифицируемый открытый ключ;

e) другие сведения, установленные уполномоченным органом.

15. В соответствии со списком, представленным руководителем органа публичной власти, и на основании заявки, полученной от служащего, в течение трех рабочих дней с даты регистрации заявки центр сертификации принимает решение о сертификации открытого ключа.

16. На основании решения о сертификации открытого ключа центром сертификации создается и выдается соответствующий сертификат открытого ключа.

17. Рассмотрение заявок на сертификацию открытых ключей, принятие решений о сертификации открытых ключей и создание сертификатов открытых ключей осуществляется в соответствии с процедурой, установленной регламентом центра сертификации.

18. Сертификат открытого ключа должен содержать:

a) отдельный регистрационный номер сертификата открытого ключа;

b) идентификационные данные центра сертификации;

c) наименование органа публичной власти и его идентификационный код IDNO;

d) фамилию и имя служащего, идентификационный номер физического лица IDNP, занимаемую должность;

e) информацию, необходимую для передачи сообщений служащему (номера телефонов, факса, адрес электронной почты);

f) открытый ключ служащего;

g) дату и время начала и окончания срока действия сертификата открытого ключа;

h) данные о криптографическом алгоритме цифровой подписи и другие технологические данные, определяемые центром сертификации;

i) сферы применения цифровой подписи, а также при необходимости предельную сумму, для которой действительно применение цифровой подписи в электронных платежных документах или при совершении сделок (в молдавских леях);

j) цифровую подпись уполномоченного лица центра сертификации;

k) другие данные в соответствии с техническими стандартами и требованиями, установленными уполномоченным органом.

19. По обращению руководителя органа публичной власти центр сертификации может указать в сертификатах открытых ключей служащих и другие сведения, не предусмотренные пунктом 18 настоящего Положения, в соответствии с законодательством.

20. Служащий обязан своевременно уведомлять ответственное подразделение и центр сертификации о любом изменении информации, содержащейся в сертификате открытого ключа.

21. Действие сертификата открытого ключа приостанавливается:

a) по решению уполномоченного органа;

b) по решению органа публичной власти;

с) при появлении оснований полагать, что нарушена конфиденциальность закрытого ключа;

д) при появлении оснований полагать, что информация, содержащаяся в сертификате открытого ключа, не соответствует действительности.

22. Сертификат открытого ключа отзывается:

а) по решению уполномоченного органа;

б) по решению органа публичной власти;

с) по письменному заявлению владельца сертификата открытого ключа;

д) в случае установленного факта компрометации закрытого ключа;

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

ф) по истечении срока, на который было приостановлено действие сертификата открытого ключа, если не было принято решение о возобновлении действия сертификата;

г) при необходимости внесения изменений в сертификат открытого ключа;

h) по истечении срока действия сертификата открытого ключа;

и) в случае увольнения или смерти владельца сертификата открытого ключа.

23. Приостановление, возобновление действия и отзыв сертификатов открытых ключей служащих осуществляется в соответствии с процедурами, установленными регламентом центра сертификации.

24. Центр сертификации определяет порядок экстренной связи с владельцем сертификата открытого ключа и ответственным подразделением в случае компрометации закрытого ключа.

25. Порядок смены открытых и закрытых ключей служащих по истечении сроков их действия устанавливается техническими нормами, утвержденными уполномоченным органом.

26. При увольнении служащего закрытый ключ данного лица уничтожается методом, который не допускает возможности его восстановления, а соответствующий сертификат открытого ключа остается действительным до истечения срока его действия.

Раздел 3. Подписание электронного документа

27. Электронные документы подписываются служащим средствами цифровой подписи с использованием своего закрытого ключа.

28. В процессе выполнения своих должностных обязанностей служащий использует свой закрытый ключ, созданный для этой цели. Использование закрытого ключа в целях, не связанных с выполнением его должностных обязанностей, запрещается.

29. Ответственное подразделение обеспечивает доступ служащих к обновленной информации о действительных, приостановленных и отозванных сертификатах открытых ключей или в ином порядке обеспечивает возможность проверки действительности сертификатов открытых ключей, выданных центром сертификации, в том числе посредством рассылки служащим измененного списка отозванных сертификатов открытых ключей, предоставляемого центром сертификации.

Раздел 4. Проверка подлинности цифровой подписи

30. Проверка подлинности цифровых подписей в электронных документах осуществляется лицом, проверяющим подлинность электронного документа, с использованием средств цифровой подписи и сертификата открытого ключа составителя документа.

III. Обязанности и права служащего

31. Служащий обязан:

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

б) использовать средства цифровой подписи в соответствии с эксплуатационной документацией и режимом применения средств цифровой подписи, установленным в органе публичной власти;

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

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

утери закрытого ключа;

имеющихся оснований полагать, что нарушена конфиденциальность закрытого ключа;

несоответствия информации, содержащейся в сертификате открытого ключа, действительности;

e) при разрешении спорных ситуаций, связанных с установлением подлинности и/или автора спорного документа, предоставлять необходимую информацию;

f) выполнять другие обязанности, установленные действующим законодательством.

32. Служащий имеет право:

a) подписывать и проверять цифровую подпись в электронных документах;

b) не принимать к исполнению электронные документы, подписанные цифровой подписью, если:

сертификат открытого ключа лица, подписавшего электронный документ, находится в списке отозванных сертификатов открытых ключей или не был действительным на момент подписания электронного документа;

не подтверждена подлинность цифровой подписи в электронном документе;

цифровая подпись используется с нарушением сферы ее применения или с превышением предельной суммы, для которой действительно применение цифровой подписи в электронных платежных документах или при совершении сделок;

c) в случае возникновения спорной ситуации, связанной с установлением подлинности и/или автора спорного документа, требовать ее разрешения в установленном порядке;

d) получать консультации по применению цифровой подписи и проверке подлинности электронного документа у персонала ответственного подразделения и центра сертификации.

IV. Обеспечение безопасности

33. Учет материальных носителей закрытых ключей осуществляется ответственным подразделением по экземплярам в соответствии с внутренним порядком применения цифровой подписи в электронных документах органа публичной власти.

34. Хранение материальных носителей закрытых ключей осуществляется в условиях, исключающих их утрату и несанкционированное использование.

35. При транспортировке материальных носителей закрытых ключей обеспечивается их защита от физических повреждений и внешних воздействий.

36. Закрытый ключ, а также, если это предусмотрено, его дубликат хранятся отдельно с обеспечением условий, при которых их одновременная компрометация невозможна.

37. Средства цифровой подписи, используемые в органе публичной власти, подлежат учету и контролю целостности ответственным подразделением. Использование средств цифровой подписи при нарушении их целостности запрещается.

38. Режим применения средств цифровой подписи в органе публичной власти должен исключать возможность доступа посторонних лиц к данным средствам, их несанкционированного использования и модификации.

V. Меры, принимаемые при компрометации закрытого ключа

39. К обстоятельствам, связанным с компрометацией закрытого ключа, относятся следующие ситуации:

a) утеря материального носителя закрытого ключа, независимо от факта его последующего обнаружения;

b) возникновение подозрений на утечку информации или ее искажение в системе связи или на местах применения средств цифровой подписи;

c) нарушение целостности печатей на хранилище с материальными носителями закрытых ключей;

d) утеря ключа от хранилища в момент нахождения в нем материальных носителей закрытых ключей, независимо от факта последующего обнаружения ключа;

e) доступ посторонних лиц к закрытому ключу или средствам цифровой

подписи;

f) другие события, которые дают основания полагать, что была нарушена конфиденциальность закрытого ключа.

40. В случае возникновения обстоятельства, связанного с компрометацией закрытого ключа, его владелец и/или ответственное подразделение обязаны в установленном порядке незамедлительно сообщить о компрометации закрытого ключа центру сертификации.

41. В течение трех рабочих дней ответственное подразделение направляет центру сертификации письменное уведомление о компрометации закрытого ключа.

42. Центр сертификации, получивший сообщение о компрометации закрытого ключа служащего, должен в установленном порядке убедиться в достоверности сообщения и незамедлительно, но не позднее трех рабочих часов, приостановить действие или отозвать сертификат соответствующего открытого ключа.

43. Действие сертификата открытого ключа приостанавливается в случаях, предусмотренных настоящим Положением, на срок, установленный уполномоченным органом. В случае, если по истечении срока, на который было приостановлено действие сертификата открытого ключа, не поступает заявка о возобновлении его действия, сертификат открытого ключа отзывается.

44. После приостановления действия или отзыва сертификата открытого ключа центр сертификации в установленном порядке направляет письменное уведомление ответственному подразделению.

45. По факту компрометации закрытого ключа проводится служебное расследование, по завершении которого, согласно решению комиссии, скомпрометированный закрытый ключ уничтожается.

46. Создание новых открытых и закрытых ключей производится после проведения расследования и устранения причин компрометации закрытого ключа.

VI. Порядок разрешения спорных ситуаций в сфере применения цифровой подписи

47. В соответствии с настоящим Положением подлежат разрешению спорные ситуации, возникшие в связи с:

- a) оспариванием целостности электронного документа;
- b) оспариванием идентификации лица, подписавшего электронный документ;
- c) оспариванием полномочий лица, подписавшего электронный документ;
- d) оспариванием действительности сертификата открытого ключа;
- e) оспариванием сферы применения цифровой подписи и иных ограничений;
- f) недоверием к средствам цифровой подписи;
- g) недоверием к центру сертификации;
- h) в иных случаях возникновения спорных ситуаций в связи с применением цифровой подписи.

48. Спорные ситуации разрешаются в рабочем порядке и/или комиссией по разрешению спорной ситуации в сфере применения цифровой подписи.

49. В случае возникновения обстоятельств, свидетельствующих о наличии спорной ситуации, стороны, вовлеченные в спор (далее – стороны), обязаны в срок не позднее одного рабочего дня проверить наличие данных обстоятельств и принять меры по разрешению спорной ситуации, известив друг друга о результатах проверки и о принятых мерах.

50. Спорная ситуация признается разрешенной в рабочем порядке в случае, если ни одна из сторон не имеет претензий.

51. В случае, если спорная ситуация не была разрешена в рабочем порядке, создается комиссия по разрешению спорной ситуации в сфере применения цифровой подписи (далее – Комиссия).

52. Комиссия по разрешению спорной ситуации в рамках органа публичной власти создается на основании решения руководителя данного органа, а в случае спорной ситуации между несколькими органами публичной власти – на основании совместного решения руководителей заинтересованных органов.

53. В состав комиссии включаются:

- a) представители сторон;
- b) сотрудники ответственных подразделений заинтересованных органов публичной власти;

- c) представитель центра сертификации;
- d) представитель уполномоченного органа;
- e) другие лица, определенные сторонами.

54. Лица, входящие в состав комиссии, должны обладать необходимыми знаниями и опытом работы в сфере применения цифровой подписи и составления электронных документов, иметь допуск к документальным материалам и программно-техническим средствам, необходимым для проведения работы комиссии.

55. Комиссия проводит работу в соответствии с регламентом о разрешении спорных ситуаций в сфере применения цифровой подписи, утвержденным уполномоченным органом.

56. В задачи комиссии входит рассмотрение на организационно-техническом уровне обстоятельств, свидетельствующих о наличии спорной ситуации, установление причин и последствий данной ситуации, определение мер, необходимых для ее разрешения.

57. В случае, если спорная ситуация признается сторонами разрешенной, то в срок не позднее пяти рабочих дней со дня окончания работы комиссии составляется акт об урегулировании спорной ситуации, который утверждается руководителями заинтересованных органов публичной власти.

58. В случае невозможности разрешения спорной ситуации в рабочем порядке или по окончании работы комиссии стороны могут обратиться в судебную инстанцию.

VII. Ответственность

59. Служащий несет персональную ответственность за обеспечение конфиденциальности своего закрытого ключа и целостность используемых средств цифровой подписи.

60. Служащий несет персональную ответственность в такой же степени, как и в случае использования собственноручной подписи.

61. При неисполнении или ненадлежащем исполнении обязательств, установленных настоящим Положением, служащие, сотрудники ответственного подразделения и центр сертификации несут ответственность согласно действующему законодательству.

Hotrrorele Guvernului

320/28.03.2006 Hotrrore pentru aprobarea Regulamentului privind ordinea de aplicare a semnrturii digitale on documentele electronice ale autorittrilor publice //Monitorul Oficial 51-54/350, 31.03.2006