

Постановление о центрах сертификации открытых ключей

№ 945 от 05.09.2005

Мониторул Официал ал Р.Молдова № 123-125/1020 от 16.09.2005

* * *

Во исполнение 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 создания и организации деятельности центров сертификации открытых ключей (прилагается).

2. Службе информации и безопасности в 6-месячный срок:
создать и обеспечить функционирование центра сертификации открытых ключей высшего уровня и центра сертификации открытых ключей органов публичного управления;

разработать и утвердить требования в сфере цифровой подписи;
разработать и представить Правительству на утверждение проект положения о порядке применения цифровой подписи в электронных документах органов публичной власти.

3. Министерству информационного развития совместно со Службой информации и безопасности в 6-месячный срок представить предложения по использованию механизмов цифровой подписи в удостоверяющих личность документах национальной паспортной системы.

4. Службе стандартизации и метрологии совместно со Службой информации и безопасности в 6-месячный срок:

организовать работы по приведению национальных стандартов в области цифровой подписи в соответствие с международными и региональными стандартами;

разработать и установить правила и процедуры подтверждения соответствия средств цифровой подписи.

5. Министерству финансов предусмотреть выделение финансовых средств на создание и обслуживание центра сертификации открытых ключей высшего уровня и центра сертификации открытых ключей органов публичного управления.

Премьер-министр
Контрассигнуют:
министр информационного развития
министр финансов

Василе ТАРЛЕВ
Владимир Моложен
Зинаида Гречаный

Кишинэу, 5 сентября 2005 г.
№ 945.

Утверждено
Постановлением Правительства
№ 945 от 5 сентября 2005 г.

ПОЛОЖЕНИЕ

**о порядке создания и организации деятельности
центров сертификации открытых ключей**

I. Общие положения

1. Положение о порядке создания и организации деятельности центров сертификации открытых ключей (в дальнейшем – положение) разработано в соответствии с Законом об электронном документе и цифровой подписи № 264-XV от 15 июля 2004 г. и устанавливает порядок создания и организации деятельности центров сертификации открытых ключей (далее – центры сертификации), их подчиненность, устанавливает требования к финансовым ресурсам центров сертификации.

2. В настоящем положении используются следующие понятия:
программно-технический комплекс – аппаратные, аппаратно-программные

и программные средства центра сертификации, которые обеспечивают выполнение функций, связанных с предоставлением услуг по сертификации открытых ключей и иных видов услуг, связанных с цифровой подписью;

уполномоченный орган – государственный орган, уполномоченный законом осуществлять разработку и реализацию государственной политики, а также осуществлять контроль в сфере применения цифровой подписи;

положение о работе центра сертификации – нормативный документ, который определяет организационные, технические и прочие условия деятельности центра сертификации при предоставлении услуг по сертификации открытых ключей.

3. Центр сертификации является юридическим лицом или подразделением юридического лица, независимо от вида собственности, оказывающим услуги по сертификации открытых ключей и иные виды услуг, связанные с цифровой подписью (в дальнейшем – услуги по сертификации открытых ключей).

4. Деятельность центра сертификации связана с областью криптографической защиты информации и осуществляется в соответствии с действующим законодательством и настоящим положением.

5. Центры сертификации создаются по следующему иерархическому принципу:

центр сертификации высшего уровня – первый уровень;

центры сертификации, предоставляющие услуги по сертификации открытых ключей третьим лицам, – второй уровень;

центры сертификации, созданные в корпоративных целях, которые не оказывают услуги по сертификации открытых ключей третьим лицам, – третий уровень.

Количество центров сертификации второго и третьего уровней не ограничивается.

II. Порядок создания центров сертификации

6. Для предоставления услуг по сертификации открытых ключей центр сертификации должен пройти процедуру регистрации в уполномоченном органе и сертифицировать открытый ключ уполномоченного лица (лиц) центра.

7. Для регистрации центра сертификации представляются следующие документы:

а) заявление о регистрации, в котором указываются:

полное наименование юридического лица, местонахождение и организационно-правовая форма;

должность, фамилия и имя руководителя юридического лица, номер документа, удостоверяющего личность, идентификационный номер физического лица IDNP;

другая контактная информация;

б) копия учредительных документов и свидетельства о государственной регистрации юридического лица;

в) банковская гарантия или страховой полис, предусмотренные пунктом 8 настоящего положения (только для центров сертификации, предоставляющих услуги по сертификации открытых ключей третьим лицам);

г) положение о работе центра сертификации, утвержденное руководителем юридического лица;

д) копия приказа руководителя юридического лица о назначении работников центра сертификации, ответственных за деятельность центра сертификации, и лиц, уполномоченных подписывать сертификаты открытых ключей, а также копии документов, удостоверяющих личность данных лиц;

е) копии документов об уровне образования и квалификации ответственных должностных лиц, функциональные обязанности которых непосредственно связаны с предоставлением услуг по сертификации открытых ключей;

ж) план-схема помещений центра сертификации и порядок доступа к помещениям специального режима;

з) порядок хранения резервных копий реестра сертификатов открытых ключей;

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

к) копия лицензии на право осуществления деятельности в сфере

криптографической защиты информации (только для центров сертификации, предоставляющих услуги по сертификации открытых ключей третьим лицам).

8. Центр сертификации, предоставляющий услуги по сертификации открытых ключей третьим лицам, обязан обладать финансовыми ресурсами, необходимыми для возмещения убытков, которые могут быть причинены владельцам сертификатов открытых ключей, пользователям или третьим лицам вследствие невыполнения или ненадлежащего выполнения центром сертификации своих обязательств.

В этих целях центр сертификации предоставляет банковскую гарантию или страховой полис в пользу уполномоченного органа на сумму, размер которой в молдавских леях эквивалентен 20000 евро.

9. На основании документов, указанных в пункте 7 настоящего положения, уполномоченный орган в срок не более 15 дней осуществляет проверку соблюдения центром сертификации требований в сфере цифровой подписи и принимает решение о регистрации или об отказе в регистрации центра сертификации.

10. В случае принятия решения о регистрации центру сертификации в течение 5 рабочих дней выдается свидетельство о регистрации.

11. Решение об отказе в регистрации должно содержать убедительное обоснование и обязательные ссылки на законодательные и нормативные акты, которые были нарушены. Решение доводится до сведения заявителя в течение 5 рабочих дней.

12. Отказ в регистрации не может служить препятствием для повторной подачи документов на регистрацию, если были устранены причины, послужившие основанием для отказа.

13. Решение об отказе в регистрации может быть обжаловано в компетентный административный суд.

14. Центр сертификации считается зарегистрированным со дня выдачи свидетельства о регистрации.

15. В случае изменения документов, указанных в пункте 7 настоящего положения, центр сертификации в течение 10 рабочих дней представляет соответствующие документы уполномоченному органу.

16. В случае уничтожения или утери свидетельства о регистрации центру сертификации выдается его дубликат в течение 5 рабочих дней со дня подачи соответствующего заявления.

17. Копия свидетельства о регистрации центра сертификации направляется Министерству информационного развития для учета центра в Государственном регистре правовых единиц.

18. Информация о зарегистрированных, а также о прекративших деятельность центрах сертификации публикуется уполномоченным органом на своей официальной странице в сети Интернет.

19. После получения свидетельства о регистрации открытый ключ уполномоченного лица центра сертификации сертифицируется в центре сертификации вышестоящего уровня в соответствии с регламентом, утвержденным уполномоченным органом.

20. Открытый ключ уполномоченного лица центра сертификации высшего уровня сертифицируется данным лицом в соответствии с регламентом работы этого центра.

21. Сертификаты открытых ключей уполномоченных лиц центров сертификации создаются в виде электронного документа и документа на бумажном носителе в двух экземплярах. Сертификат открытого ключа в виде документа на бумажном носителе собственноручно подписывается владельцем сертификата открытого ключа и уполномоченным лицом вышестоящего центра сертификации и заверяется печатью. Один экземпляр сертификата открытого ключа передается уполномоченному лицу центра сертификации, а другой хранится в вышестоящем центре сертификации.

III. Организация деятельности центров сертификации

22. Центр сертификации предоставляет услуги по сертификации открытых ключей в соответствии с процедурами сертификации открытых ключей и положением о работе центра сертификации.

23. Центр сертификации предоставляет следующие основные виды услуг по сертификации открытых ключей:

- a) сертификация открытых ключей уполномоченных лиц нижестоящих центров сертификации;
- b) сертификация открытых ключей физических лиц;
- c) сертификация открытых ключей услуг, предоставляемых в информационной сфере;
- d) фиксирование времени подписания электронного документа.

24. Центр сертификации, созданный в корпоративных целях, не может сертифицировать открытые ключи уполномоченных лиц центров сертификации других юридических лиц.

25. Центр сертификации может предоставлять и иные виды услуг, связанные с цифровой подписью.

26. Центры сертификации второго уровня предоставляют услуги по сертификации открытых ключей на договорной основе.

27. Центр сертификации обязан:

- a) осуществлять свою деятельность в соответствии с законодательством и регламентациями уполномоченного органа, изданными в пределах его компетенции;

- b) принимать необходимые меры по обеспечению безопасности и защите информации в процессе предоставления услуг по сертификации открытых ключей;

- c) размещать программно-технический комплекс, предназначенный для предоставления услуг по сертификации открытых ключей, в специальных помещениях и обеспечивать их охрану;

- d) располагать персоналом, обладающим необходимой квалификацией для предоставления услуг по сертификации открытых ключей;

- e) проверять достоверность данных, указанных в заявке на сертификацию открытого ключа, на основании документов, подтверждающих указанные данные;

- f) информировать владельца сертификата открытого ключа об ограничениях по использованию цифровой подписи и порядке возмещения убытков;

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

- h) вести реестр сертификатов открытых ключей, обеспечивать его актуализацию и свободный доступ к реестру;

- i) создавать и хранить резервную копию реестра сертификатов открытых ключей в соответствии с требованиями, утвержденными уполномоченным органом;

- j) включать сертификат открытого ключа в реестр сертификатов открытых ключей не позднее даты и времени начала действия сертификата;

- k) обеспечивать возможность определения даты и времени выдачи, приостановления действия или отзыва сертификата открытого ключа, представлять другую имеющуюся информацию для подтверждения подлинности цифровой подписи;

- l) приостанавливать действие сертификата открытого ключа или отзывать его в случаях, установленных законом, и вносить соответствующие изменения в реестр сертификатов открытых ключей в установленные сроки;

- m) уведомлять владельца сертификата открытого ключа о ставших известными центру сертификации фактах, указывающих на невозможность дальнейшего использования закрытого ключа, а также об отзыве сертификата открытого ключа;

- n) хранить всю информацию о сертификате открытого ключа не менее десяти лет с момента отзыва сертификата;

- o) выполнять иные обязанности, предусмотренные законодательством и заключенными договорами.

28. В процессе формирования сертификата открытого ключа центр сертификации:

- a) присваивает уникальный регистрационный номер сертификату;

- b) проверяет уникальность открытого ключа в реестре сертификатов открытых ключей;

- c) при необходимости включает данные об ограничениях по использованию сертификата открытого ключа или об ограничениях стоимости сделок, в которых он может использоваться;

d) включает электронный адрес реестра сертификатов открытых ключей для обеспечения доступа к реестру;

e) по просьбе владельца сертификата открытого ключа может указывать в сертификате дополнительные сведения, при условии, что они не противоречат законодательству, не создают угрозу национальной безопасности или общественному порядку, и только после предварительной проверки точности этих сведений.

29. Обязательными должностями в центре сертификации являются: администратор регистрации, администратор сертификации, администратор безопасности и системный администратор. По решению руководителя юридического лица могут быть созданы и другие должности.

30. Администратор регистрации отвечает за правильность информационного наполнения сертификата открытого ключа и регистрацию владельцев сертификатов открытых ключей в процессе создания, приостановления и возобновления действия, а также отзыва сертификатов.

31. Администратор сертификации (уполномоченное лицо центра сертификации) отвечает за создание и отзыв сертификатов открытых ключей, ведение реестра сертификатов открытых ключей, безопасное хранение и использование своего закрытого ключа.

32. Администратор безопасности отвечает за надлежащее функционирование комплексной системы защиты информации.

33. Системный администратор отвечает за функционирование программно-технического комплекса и обеспечение его безопасности.

34. Совмещение указанных должностей с другими должностями запрещается.

35. По окончании срока действия сертификата открытого ключа уполномоченного лица центра сертификации соответствующий закрытый ключ цифровой подписи и все его резервные копии уничтожаются методом, который не допускает возможности их восстановления. Уничтожение осуществляется специальной комиссией с оформлением акта об уничтожении закрытого ключа.

IV. Центр сертификации открытых ключей высшего уровня

36. Центр сертификации открытых ключей высшего уровня создается и обслуживается Службой информации и безопасности и предназначен для сертификации открытых ключей уполномоченных лиц центров сертификации второго уровня.

37. Положение о работе центра сертификации открытых ключей высшего уровня утверждается директором Службы информации и безопасности.

38. Центр сертификации открытых ключей высшего уровня выполняет следующие функции:

a) сертифицирует открытые ключи уполномоченных лиц центров сертификации второго уровня;

b) приостанавливает, возобновляет действие и отзывает сертификаты открытых ключей, выданные этим центром;

c) создает и ведет реестр сертификатов открытых ключей уполномоченных лиц центров сертификации второго уровня;

d) подтверждает подлинность и действительность сертификатов открытых ключей уполномоченных лиц центров сертификации второго уровня.

39. В процессе своей деятельности центр сертификации открытых ключей высшего уровня может взаимодействовать с центрами сертификации других государств и участвовать в создании межгосударственных и международных систем инфраструктуры открытых ключей.

40. Деятельность центра сертификации открытых ключей высшего уровня финансируется за счет средств государственного бюджета, а также из других разрешенных законом источников финансирования.

V. Центр сертификации открытых ключей органов публичного управления

41. Центр сертификации открытых ключей органов публичного управления создается и обслуживается государственным предприятием "Центр специальных коммуникаций" Службы информации и безопасности и предназначен для обеспечения применения цифровой подписи в электронных документах органов публичного управления Республики Молдова.

42. Положение о работе центра сертификации открытых ключей органов публичного управления утверждается директором Службы информации и безопасности.

43. Центр сертификации открытых ключей органов публичного управления является центром сертификации второго уровня и выполняет следующие функции:

- a) сертифицирует открытые ключи ответственных должностных лиц и других работников органов публичного управления;
- b) участвует в обеспечении безопасного доступа к государственным информационным услугам и ресурсам;
- c) выполняет иные функции, связанные с цифровой подписью.

44. Центр сертификации открытых ключей органов публичного управления может предоставлять на договорной основе услуги по сертификации открытых ключей третьим лицам в соответствии с положениями разделов II и III настоящего положения.

45. Деятельность центра сертификации открытых ключей органов публичного управления финансируется за счет средств государственного бюджета, а также за счет других разрешенных законом источников финансирования.

VI. Прекращение деятельности центров сертификации

46. Деятельность центра сертификации может быть прекращена в установленном законодательством порядке, в том числе по инициативе уполномоченного органа, в следующих случаях:

- a) принятие юридическим лицом решения о прекращении деятельности центра сертификации;
- b) аннулирование банковской гарантии или страхового полиса, предусмотренных пунктом 8 настоящего положения;
- c) нарушение центром сертификации законодательства о цифровой подписи;
- d) невыполнение центром сертификации требований в сфере цифровой подписи, утвержденных уполномоченным органом;
- e) другие случаи, предусмотренные законодательством.

47. В случае принятия решения о прекращении деятельности центра сертификации свидетельство о регистрации аннулируется.

Аннулирование свидетельства о регистрации не влечет за собой отзыв лицензии на право осуществления деятельности в области криптографической защиты информации.

48. Все сертификаты открытых ключей, выданные центром сертификации, деятельность которого прекращается, отзываются и передаются на хранение другому центру сертификации в установленном уполномоченным органом порядке за счет средств центра сертификации, прекращающего свою деятельность.

49. Сведения о прекращении деятельности центра сертификации вносятся в Государственный регистр правовых единиц с указанием оснований прекращения деятельности.

50. Решение о прекращении деятельности центра сертификации может быть обжаловано в судебном порядке.