

Утверждено:  
Служба информации и  
безопасности Республики Молдова  
приказ № 13 от 3 апреля 2006 г.

Зарегистрировано:  
Министерство юстиции  
Республики Молдова  
рег. номер 452 от 21 июня 2006 г.

\_\_\_\_\_ Ион УРСУ

\_\_\_\_\_ Виктория ИФТОДИ

Приложение № 3  
к Приказу директора Службы  
информации и безопасности  
Республики Молдова  
№ 13 от 3 апреля 2006 г.

## **РЕГЛАМЕНТ**

### **Центра сертификации открытых ключей высшего уровня**

#### **I. Общие положения**

1. Настоящий регламент разработан на основании Закона об электронном документе и цифровой подписи № 264-XV от 15 июля 2004 г. и Постановления Правительства № 945 от 5 сентября 2005 г. "О центрах сертификации открытых ключей".

2. Регламент устанавливает общие условия организации деятельности Центра сертификации открытых ключей высшего уровня (далее – Центр сертификации), определяет его функции, обязанности и права, процедуры и механизмы, применяемые Центром сертификации для управления единой иерархической инфраструктурой открытых ключей (Public Key Infrastructure, PKI), а также общий порядок взаимодействия с центрами сертификации и пользователями цифровой подписи, основные организационно-технические мероприятия по обеспечению безопасности.

3. Регламент Центра сертификации открытых ключей высшего уровня является нормативным актом в сфере применения цифровой подписи, обязательным для всех физических и юридических лиц, применяющих цифровую подпись или осуществляющих деятельность в сфере цифровой подписи.

4. Центр сертификации является подразделением Службы информации и безопасности, осуществляющим деятельность в сфере криптографической и технической защиты информации.

5. Руководитель Центра сертификации назначается приказом директора Службы информации и безопасности.

#### **II. Функции, обязанности и права Центра сертификации**

6. Центр сертификации выполняет следующие функции:
- а) сертифицирует открытые ключи уполномоченных лиц центров сертификации второго уровня;
  - б) приостанавливает, возобновляет действие и отзывает сертификаты открытых ключей, выданные Центром сертификации;

с) создает и ведет реестр сертификатов открытых ключей уполномоченных лиц Центра сертификации и центров сертификации второго уровня (далее – Реестр сертификатов открытых ключей);

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

7. Во исполнение возложенных на него функций Центр сертификации:

a) обеспечивает создание и выдачу сертификатов открытых ключей уполномоченным лицам центров сертификации второго уровня в форме электронного документа и в виде документа на бумажном носителе, по их заявке, в соответствии с процедурами, установленными настоящим Регламентом;

b) приостанавливает, возобновляет действие и отзывает сертификаты открытых ключей уполномоченных лиц центров сертификации второго уровня в случаях и в соответствии с процедурами, установленными настоящим Регламентом;

с) ведет учет центров сертификации второго уровня;

d) ведет Реестр сертификатов открытых ключей в виде документов на бумажном носителе и в форме электронных документов;

e) обеспечивает взаимодействие с центрами сертификации второго уровня в рамках единой иерархической инфраструктуры открытых ключей;

f) оказывает консультационную и методологическую помощь уполномоченным лицам центров сертификации второго уровня;

g) подтверждает подлинность и действительность сертификатов открытых ключей уполномоченных лиц центров сертификации второго уровня;

h) подтверждает подлинность и действительность сертификатов открытых ключей, выданных центрами сертификации второго уровня, в случаях, предусмотренных настоящим Регламентом;

i) осуществляет деятельность в сфере криптографической и технической защиты информации;

j) создает информационные и телекоммуникационные системы Центра сертификации, обеспечивает их функционирование, безопасность, обслуживание и совершенствование, осуществляет постоянный внутренний аудит безопасности и функциональности этих систем.

8. Центр сертификации обязан:

осуществлять свою деятельность в строгом соответствии с законодательством и требованиями, установленными уполномоченным органом по разработке и реализации государственной политики и контролю в сфере применения цифровой подписи (далее – уполномоченный орган);

использовать средства цифровой подписи, имеющие сертификат соответствия, выданный в соответствии с действующим законодательством;

использовать средства цифровой подписи в соответствии с эксплуатационной документацией;

организовать внутренний режим работы Центра сертификации таким образом, чтобы исключить возможность доступа посторонних лиц к средствам цифровой подписи, их несанкционированного использования и модификации;

обеспечивать безопасность закрытых ключей уполномоченных лиц Центра сертификации и других сотрудников, создавать необходимые условия для исключения несанкционированного доступа к закрытым ключам;

управлять материальными носителями закрытых ключей в соответствии с требованиями, установленными уполномоченным органом;

использовать закрытый ключ уполномоченного лица Центра сертификации только для подписания выдаваемых им сертификатов открытых ключей и списков отозванных сертификатов;

создавать сертификат открытого ключа уполномоченного лица Центра сертификации и список отозванных сертификатов в соответствии с требованиями, установленными уполномоченным органом и настоящим Регламентом;

не использовать для создания цифровой подписи закрытый ключ при наличии оснований (подозрений) полагать, что нарушена конфиденциальность закрытого ключа;

немедленно приостановить действие сертификата открытого ключа уполномоченного лица Центра сертификации при наличии оснований (подозрений) полагать, что нарушена конфиденциальность закрытого ключа, а также в случае, если содержащаяся в сертификате открытого ключа информация не соответствует действительности;

отозвать сертификат открытого ключа уполномоченного лица Центра сертификации в случае установленного факта нарушения конфиденциальности закрытого ключа или несоответствия действительности информации, содержащейся в сертификате открытого ключа;

принимать заявки на сертификацию открытых ключей от уполномоченных лиц центров сертификации второго уровня в соответствии с процедурами, установленными настоящим Регламентом;

проверять достоверность данных, указанных в заявке на сертификацию открытого ключа, на основании документов, подтверждающих указанные данные, обеспечивать соответствие информации, содержащейся в сертификате открытого ключа, информации, представленной уполномоченным лицом центра сертификации второго уровня;

обеспечивать уникальность регистрационной информации уполномоченных лиц центров сертификации второго уровня в Реестре сертификатов открытых ключей;

не разглашать конфиденциальную и иную охраняемую законом информацию;

проверять уникальность сертифицируемых открытых ключей;

обеспечивать уникальность регистрационных номеров выдаваемых сертификатов открытых ключей;

создавать сертификат открытого ключа уполномоченного лица центра сертификации второго уровня в соответствии с требованиями, установленными уполномоченным органом и настоящим Регламентом;

вносить сертификат открытого ключа в Реестр сертификатов открытых ключей не позднее даты и времени начала действия сертификата;

выдавать сертификаты открытых ключей уполномоченным лицам центров сертификации второго уровня в соответствии с процедурами, установленными настоящим Регламентом;

приостанавливать, возобновлять действие или отзывать сертификат открытого ключа уполномоченного лица центра сертификации второго уровня в случаях и в соответствии с процедурами, установленными настоящим Регламентом;

вносить сведения об отозванном или приостановленном сертификате открытого ключа в список отозванных сертификатов в течение 3 рабочих часов с указанием даты и времени внесения и причины отзыва или приостановления действия сертификата;

исключать сведения о приостановленном сертификате открытого ключа из списка отозванных сертификатов в течение 3 рабочих часов с момента возобновления его действия;

заранее уведомлять уполномоченное лицо центра сертификации второго уровня о приостановлении действия или об отзыве сертификата открытого ключа в случаях и в соответствии с процедурами, установленными настоящим Регламентом;

уведомлять уполномоченное лицо центра сертификации второго уровня о приостановлении, возобновлении действия или отзыве его сертификата открытого ключа в соответствии с процедурами, установленными настоящим Регламентом;

уведомлять уполномоченное лицо центра сертификации второго уровня о фактах, ставших известными Центру сертификации, которые существенным образом могут повлиять на возможность дальнейшего использования сертификата открытого ключа уполномоченного лица центра сертификации второго уровня;

уведомлять владельца сертификата открытого ключа о ставших известными Центру сертификации фактах, указывающих на невозможность дальнейшего использования закрытого ключа, принадлежащего данному владельцу;

хранить сертификат открытого ключа уполномоченного лица центра сертификации второго уровня, а также иную информацию о данном сертификате не менее 10 лет с момента отзыва или окончания срока действия сертификата;

обеспечивать актуальность Реестра сертификатов открытых ключей и возможность свободного доступа к нему уполномоченных лиц центров сертификации второго уровня и пользователей цифровой подписи, принимать необходимые меры по обеспечению безопасности Реестра;

предоставлять уполномоченным лицам центров сертификации второго уровня и пользователям цифровой подписи сведения из Реестра сертификатов открытых ключей об отозванных или приостановленных сертификатах;

создавать и хранить резервную копию Реестра сертификатов открытых ключей в соответствии с требованиями, установленными уполномоченным органом;

обеспечивать возможность определения даты и времени выдачи, приостановления действия и отзыва сертификата открытого ключа;

подтверждать подлинность и действительность сертификатов открытых ключей уполномоченных лиц центров сертификации второго уровня по обращениям пользователей цифровой подписи;

по запросу судебной инстанции, а также лиц и органов, имеющих такое право в силу закона, или в других случаях, предусмотренных законодательством в сфере применения цифровой подписи, подтверждать подлинность и действительность сертификатов открытых ключей, выданных центрами сертификации второго уровня, и предоставлять копии сертификатов открытых ключей, находящихся в Реестре сертификатов открытых ключей, на бумажном носителе;

синхронизировать работу служб Центра сертификации, в том числе программных и технических средств по назначению, с Всемирным координированным временем (UTC). Допускается синхронизация служб с Гринвичским средним временем (Greenwich Mean Time, GMT), без учета перехода на летнее время;

размещать программно-технические средства, предназначенные для сертификации открытых ключей, в специальных помещениях и обеспечивать их безопасность;

располагать персоналом, обладающим необходимой квалификацией.

9. Центр сертификации имеет право:

а) создавать сертификат открытого ключа уполномоченного лица Центра сертификации и выполнять процедуру самовыдачи сертификата открытого ключа;

б) назначать несколько уполномоченных лиц, имеющих равные полномочия по подписанию сертификатов открытых ключей уполномоченных лиц центров сертификации второго уровня;

в) отказать в выдаче сертификата открытого ключа уполномоченному лицу центра сертификации второго уровня с указанием причин отказа в случаях:

представления в заявке на сертификацию открытого ключа информации, не соответствующей действительности;

нарушения положений законодательства в сфере применения цифровой подписи;

нарушения прав третьих лиц в процессе составления или подачи заявки;

д) подтверждать подлинность и действительность сертификатов открытых ключей пользователей цифровой подписи;

е) приостановить действие или отозвать сертификат открытого ключа уполномоченного лица центра сертификации второго уровня в случаях и в порядке, предусмотренных законодательством и настоящим Регламентом.

### III. Организация работы Центра сертификации

#### *Раздел 1. Процедуры Центра сертификации*

10. Центр сертификации выполняет следующие процедуры:

- a) сертификация открытого ключа уполномоченного лица Центра сертификации;
- b) приостановление действия сертификата открытого ключа уполномоченного лица Центра сертификации;
- c) отзыв сертификата открытого ключа уполномоченного лица Центра сертификации;
- d) сертификация открытого ключа уполномоченного лица центра сертификации второго уровня;
- e) приостановление действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня;
- f) отзыв сертификата открытого ключа уполномоченного лица центра сертификации второго уровня;
- g) подтверждение подлинности и действительности сертификата открытого ключа.

#### *1.1. Сертификация открытого ключа уполномоченного лица Центра сертификации*

11. Создание сертификата открытого ключа уполномоченного лица Центра сертификации осуществляется самим Центром сертификации на основании полномочий, установленных законодательством в сфере применения цифровой подписи.

12. Уполномоченное лицо Центра сертификации создает свои открытый и закрытый ключи в соответствии с требованиями, установленными уполномоченным органом.

13. Уполномоченное лицо Центра сертификации создает сертификат открытого ключа в форме электронного документа и подписывает его своим закрытым ключом.

14. Сертификат открытого ключа уполномоченного лица Центра сертификации в форме электронного документа должен соответствовать стандарту ISO/IEC 9594/8 Directory Services, стандарту Международного союза телекоммуникаций ITU-T X.509, версия 3, и рекомендации IETF (Internet Engineering Task Force) RFC 3280 (RFC 2459).

15. После создания сертификата открытого ключа в форме электронного документа уполномоченное лицо Центра сертификации создает сертификат открытого ключа в виде документа на бумажном носителе, который должен содержать:

- a) регистрационный номер сертификата открытого ключа;
- b) идентификационные данные Центра сертификации, идентификационный номер правовой единицы (IDNO);

- c) фамилию и имя уполномоченного лица Центра сертификации – владельца сертификата открытого ключа;
- d) идентификационный номер физического лица – уполномоченного лица Центра сертификации (IDNP);
- e) наименование Центра сертификации и занимаемую должность уполномоченного лица Центра сертификации;
- f) открытый ключ уполномоченного лица Центра сертификации – владельца сертификата открытого ключа;
- 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 и иные установленные ограничения;
- j) другие данные в соответствии с техническими стандартами и требованиями, установленными уполномоченным органом.

16. Структура сертификата открытого ключа уполномоченного лица Центра сертификации представлена в приложении № 1 к настоящему Регламенту.

17. Сертификат открытого ключа уполномоченного лица Центра сертификации на бумажном носителе подписывается уполномоченным лицом Центра сертификации, руководителем Центра сертификации, утверждается директором Службы информации и безопасности и заверяется печатью Службы.

18. Сертификат открытого ключа уполномоченного лица Центра сертификации в форме электронного документа является действительным при условии, что:

- a) содержащаяся в сертификате информация соответствует информации, указанной в утвержденном сертификате на бумажном носителе;
- b) сертификат подписан закрытым ключом уполномоченного лица Центра сертификации, соответствующим открытому ключу, содержащемуся в сертификате.

19. В целях международного признания сертификатов открытых ключей, выданных в инфраструктуре открытых ключей Республики Молдова, допускается сертификация открытого ключа уполномоченного лица Центра сертификации в центре сертификации международного уровня.

20. Сертификат открытого ключа уполномоченного лица Центра сертификации хранится в Реестре сертификатов открытых ключей в виде документа на бумажном носителе и в форме электронного документа.

## *1.2. Приостановление действия сертификата открытого ключа уполномоченного лица Центра сертификации*

21. Приостановление действия сертификата открытого ключа уполномоченного лица Центра сертификации осуществляется по решению уполномоченного органа в случае:

- а) нарушения законодательства в сфере применения цифровой подписи;
- б) наличия оснований полагать, что нарушена конфиденциальность закрытого ключа; или
- в) наличия оснований полагать, что информация, содержащаяся в сертификате открытого ключа, не соответствует действительности.

22. Действие сертификата открытого ключа уполномоченного лица Центра сертификации приостанавливается распоряжением директора Службы информации и безопасности на срок до 30 дней.

23. Сертификат открытого ключа уполномоченного лица Центра сертификации, действие которого приостановлено, в течение 3 рабочих часов помещается в список отозванных сертификатов Центра сертификации, а Центр сертификации выпускает обновленный список отозванных сертификатов.

24. Временем приостановления действия сертификата открытого ключа уполномоченного лица Центра сертификации считается время опубликования (выпуска) обновленного списка отозванных сертификатов (время, указанное в поле This Update).

25. Список отозванных сертификатов Центра сертификации является электронным документом и должен соответствовать стандарту ISO/IEC 9594/8 Directory Services, стандарту Международного союза телекоммуникаций ITU-T X.509, версия 2, и рекомендации IETF RFC 3280 (RFC 2459).

26. Структура списка отозванных сертификатов представлена в Приложении № 2 к настоящему Регламенту.

27. В случае приостановления действия сертификата открытого ключа уполномоченного лица Центра сертификации, распоряжением директора Службы информации и безопасности создается комиссия для проведения служебного расследования.

28. В состав комиссии должны входить:

- а) представители уполномоченного органа;
- б) руководитель Центра сертификации;
- в) другие лица, обладающие необходимыми знаниями и опытом работы в сфере применения цифровой подписи и составления электронных документов.

29. Лица, входящие в состав комиссии, должны иметь допуск к документальным материалам и программно-техническим средствам, необходимым для проведения работы комиссии.

30. Комиссия рассматривает, на организационно-техническом уровне, обстоятельства, повлекшие за собой приостановление действия сертификата открытого ключа уполномоченного лица Центра сертификации, устанавливает причины и последствия данной ситуации, определяет меры, необходимые для ее разрешения.

31. Срок работы комиссии должен составлять не более 30 дней с момента приостановления действия сертификата открытого ключа уполномоченного лица Центра сертификации.

32. В срок не позднее, чем за 5 дней до даты окончания срока, на который было приостановлено действие сертификата открытого ключа уполномоченного лица Центра сертификации, комиссией оформляется акт с указанием обстоятельств, повлекших за собой приостановление действия сертификата открытого ключа, установленных причин и последствий данной ситуации, мер, необходимых для ее разрешения, и рекомендаций по возобновлению действия или отзыву сертификата открытого ключа уполномоченного лица Центра сертификации.

33. По результатам работы комиссии, в срок не более чем за 5 дней до даты окончания срока, на который было приостановлено действие сертификата открытого ключа уполномоченного лица Центра сертификации, распоряжением директора Службы информации и безопасности принимается решение о возобновлении действия или об отзыве сертификата открытого ключа уполномоченного лица Центра сертификации.

34. В случае, если до истечения срока, на который было приостановлено действие сертификата открытого ключа, не принимается решение о возобновлении его действия, сертификат открытого ключа отзывается.

35. Сертификат открытого ключа уполномоченного лица Центра сертификации, действие которого возобновлено, в течение 3 рабочих часов исключается из списка отозванных сертификатов, а Центром сертификации выпускается обновленный список отозванных сертификатов.

36. Временем возобновления действия сертификата открытого ключа уполномоченного лица Центра сертификации считается время опубликования (выпуска) обновленного списка отозванных сертификатов (время, указанное в поле This Update).

### *1.3. Отзыв сертификата открытого ключа уполномоченного лица Центра сертификации*

37. Сертификат открытого ключа уполномоченного лица Центра сертификации отзывается по решению уполномоченного органа:

- a) в случае установленного факта компрометации закрытого ключа;
- b) при обнаружении несоответствия действительности сведений, указанных в заявке на сертификацию открытого ключа или в сертификате открытого ключа;
- c) при внесении изменений в сертификат открытого ключа;
- d) по истечении срока, на который было приостановлено действие сертификата открытого ключа, если не было принято решение об его возобновлении;
- e) по истечении срока действия сертификата открытого ключа.

38. Отзыв сертификата открытого ключа уполномоченного лица Центра сертификации по причинам, указанным в подпунктах a) и b) пункта 37

настоящего Регламента, осуществляется только после предварительного приостановления его действия.

39. Решение об отзыве сертификата открытого ключа уполномоченного лица Центра сертификации оформляется в виде распоряжения директора Службы информации и безопасности.

40. Отозванный сертификат открытого ключа уполномоченного лица Центра сертификации в течение 3 рабочих часов помещается в список отозванных сертификатов, а Центром сертификации выпускается обновленный список отозванных сертификатов.

41. Временем отзыва сертификата открытого ключа уполномоченного лица Центра сертификации считается время опубликования (выпуска) обновленного списка отозванных сертификатов (время, указанное в поле This Update).

42. В случае отзыва сертификата открытого ключа по причине истечения срока его действия, данный сертификат в список отозванных сертификатов не помещается.

43. В случае увольнения уполномоченного лица Центра сертификации его закрытый ключ уничтожается без нарушения конфиденциальности ключа комиссией, назначенной распоряжением директора Службы информации и безопасности, а сертификат соответствующего открытого ключа продолжает действовать до истечения срока его действия.

#### *1.4. Сертификация открытого ключа уполномоченного лица центра сертификации второго уровня*

44. После получения свидетельства о регистрации центра сертификации второго уровня уполномоченное лицо данного центра создает свои открытый и закрытый ключи в соответствии с требованиями, установленными уполномоченным органом.

45. Открытый ключ уполномоченного лица центра сертификации второго уровня сертифицируется Центром сертификации в соответствии с настоящим Регламентом.

46. Для сертификации открытого ключа уполномоченного лица центра сертификации второго уровня данное лицо лично представляет в Центр сертификации следующие документы и информацию:

а) заявку на сертификацию открытого ключа уполномоченного лица центра сертификации второго уровня в виде документа на бумажном носителе, подписанного собственноручной подписью (приложение № 3 к настоящему Регламенту);

б) заявку на сертификацию открытого ключа уполномоченного лица центра сертификации второго уровня в форме электронного документа, подписанного цифровой подписью уполномоченного лица центра сертификации второго уровня с использованием закрытого ключа, соответствующего сертифицируемому открытому ключу – на материальном носителе;

- c) свидетельство о регистрации центра сертификации второго уровня;
- d) приказ руководителя центра сертификации второго уровня о назначении уполномоченного лица данного центра;
- e) удостоверение личности уполномоченного лица центра сертификации второго уровня;
- f) материальный носитель сертификата открытого ключа в форме электронного документа, соответствующий требованиям, установленным уполномоченным органом.

47. Заявка на сертификацию открытого ключа уполномоченного лица центра сертификации второго уровня должна содержать:

- a) фамилию и имя уполномоченного лица центра сертификации второго уровня, номер документа, удостоверяющего его личность;
- b) информацию, необходимую для связи с уполномоченным лицом центра сертификации второго уровня (номер телефона, факса, почтовый адрес, адрес электронной почты);
- c) наименование и реквизиты юридического лица, создавшего центр сертификации второго уровня;
- d) наименование и другие данные о центре сертификации второго уровня;
- e) сертифицируемый открытый ключ.

48. Заявка на сертификацию открытого ключа уполномоченного лица центра сертификации второго уровня в форме электронного документа должна соответствовать стандарту PKCS#10: Certification Request Syntax Specification Version 1.7 и рекомендации IETF (Internet Engineering Task Force) RFC 2986 Certification Request Syntax Specification.

49. Структура заявки на сертификацию открытого ключа уполномоченного лица центра сертификации второго уровня в форме электронного документа представлена в приложении № 4 к настоящему Регламенту.

50. Администратор регистрации Центра сертификации идентифицирует уполномоченное лицо центра сертификации второго уровня на основании поданных документов и осуществляет предварительную проверку.

51. В процессе осуществления предварительной проверки администратор регистрации должен установить выполнение следующих условий:

- a) соблюдение заявителем положений действующего законодательства в сфере применения цифровой подписи при составлении и подаче заявки на сертификацию открытого ключа;
- b) соблюдение заявителем прав третьих лиц при составлении и подаче заявки на сертификацию открытого ключа;
- c) соответствие информации, представленной в заявке на сертификацию открытого ключа в форме электронного документа, информации, представленной в соответствующей заявке в виде документа на бумажном носителе;
- d) действительность информации, представленной в заявке на сертификацию открытого ключа.

52. В случае выполнения заявителем всех условий, предусмотренных в пункте 51 настоящего Регламента, администратор регистрации Центра сертификации регистрирует уполномоченное лицо центра сертификации второго уровня. В противном случае, администратор регистрации Центра сертификации отказывает уполномоченному лицу центра сертификации второго уровня в регистрации и возвращает заявителю поданные документы.

53. Решение об отказе в регистрации уполномоченного лица центра сертификации второго уровня может быть обжаловано в уполномоченном органе или в судебном порядке и не служит препятствием для повторной подачи заявки, если были устранены причины, послужившие основанием для отказа в регистрации.

54. В случае регистрации уполномоченного лица центра сертификации второго уровня администратор регистрации Центра сертификации передает уполномоченному лицу Центра сертификации (администратору сертификации) следующие документы:

а) зарегистрированную и заверенную собственноручной подписью администратора регистрации заявку на сертификацию открытого ключа уполномоченного лица центра сертификации второго уровня в виде документа на бумажном носителе;

б) зарегистрированную заявку на сертификацию открытого ключа уполномоченного лица центра сертификации второго уровня в форме электронного документа, подписанного цифровой подписью администратора регистрации;

с) зарегистрированную администратором регистрации копию приказа руководителя центра сертификации второго уровня о назначении уполномоченного лица данного центра;

д) зарегистрированную администратором регистрации копию свидетельства о регистрации центра сертификации второго уровня;

е) зарегистрированную администратором регистрации копию удостоверения личности уполномоченного лица центра сертификации второго уровня;

ф) материальный носитель сертификата открытого ключа, соответствующий требованиям, установленным уполномоченным органом.

55. Уполномоченное лицо Центра сертификации (администратор сертификации) в течение 3 рабочих дней с даты регистрации заявки принимает решение о сертификации открытого ключа уполномоченного лица центра сертификации второго уровня.

56. В случае выявления нарушений законодательства в сфере применения цифровой подписи уполномоченное лицо Центра сертификации принимает решение об отказе в сертификации открытого ключа, с обязательным указанием причин отказа.

57. Решение об отказе в сертификации открытого ключа может быть обжаловано в уполномоченном органе или в судебном порядке и не служит препятствием для повторной подачи заявки, если были устранены причины, послужившие основанием для отказа.

58. В случае положительного решения о сертификации открытого ключа уполномоченное лицо Центра сертификации создает сертификат открытого ключа уполномоченного лица центра сертификации второго уровня в виде документа на бумажном носителе в двух экземплярах.

59. Сертификат открытого ключа уполномоченного лица центра сертификации второго уровня должен содержать:

- a) регистрационный номер сертификата открытого ключа;
- b) идентификационные данные центра сертификации второго уровня, IDNO;
- c) фамилию и имя уполномоченного лица центра сертификации второго уровня – владельца сертификата открытого ключа;
- d) идентификационный номер физического лица – уполномоченного лица центра сертификации второго уровня (IDNP);
- e) наименование центра сертификации и занимаемую должность уполномоченного лица центра сертификации второго уровня;
- f) информацию, необходимую для связи с уполномоченным лицом центра сертификации второго уровня – владельцем сертификата открытого ключа;
- g) открытый ключ уполномоченного лица центра сертификации второго уровня – владельца сертификата открытого ключа;
- h) дату и время начала и окончания срока действия сертификата открытого ключа;
- i) данные о криптографическом алгоритме цифровой подписи и другие технологические данные, определяемые Центром сертификации;
- j) сферы применения цифровой подписи и иные установленные ограничения;
- k) цифровую подпись уполномоченного лица Центра сертификации;
- l) другие данные, в соответствии с техническими стандартами и требованиями, установленными уполномоченным органом.

60. Сертификат открытого ключа уполномоченного лица центра сертификации второго уровня в форме электронного документа должен соответствовать стандарту ISO/IEC 9594/8 Directory Services, стандарту Международного союза телекоммуникаций ITU-T X.509, версия 3, и рекомендации IETF (Internet Engineering Task Force) RFC 3280 (RFC 2459).

61. Структура сертификата открытого ключа уполномоченного лица центра сертификации второго уровня представлена в приложении № 5 к настоящему Регламенту.

62. Уполномоченное лицо Центра сертификации создает сертификат открытого ключа уполномоченного лица центра сертификации второго уровня в форме электронного документа, соответствующий сертификату на бумажном носителе, и подписывает его цифровой подписью.

63. Сертификат открытого ключа уполномоченного лица центра сертификации второго уровня в форме электронного документа является действительным при условии, что он содержит информацию, соответствующую

информации, содержащейся в соответствующем сертификате на бумажном носителе.

64. Срок действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня – 5 лет.

65. Администратор регистрации Центра сертификации уведомляет уполномоченное лицо центра сертификации второго уровня о создании сертификата его открытого ключа.

66. Сертификат открытого ключа уполномоченного лица центра сертификации второго уровня в виде документа на бумажном носителе в двух экземплярах подписывается собственноручными подписями уполномоченным лицом Центра сертификации и уполномоченным лицом центра сертификации второго уровня и заверяется печатями Центра сертификации и центра сертификации второго уровня.

67. Уполномоченному лицу центра сертификации второго уровня выдаются:

а) один экземпляр подписанного и заверенного печатями сертификата открытого ключа уполномоченного лица центра сертификации второго уровня в виде документа на бумажном носителе;

б) копия сертификата открытого ключа уполномоченного лица Центра сертификации в виде документа на бумажном носителе;

в) материальный носитель, содержащий следующие электронные документы:

сертификат открытого ключа уполномоченного лица центра сертификации второго уровня;

сертификат открытого ключа уполномоченного лица Центра сертификации;

обновленную версию списка отозванных сертификатов;

д) документ на бумажном носителе, содержащий идентификационные данные уполномоченного лица центра сертификации второго уровня и ключевую фразу для его удаленной аутентификации.

68. Сертификат открытого ключа уполномоченного лица центра сертификации второго уровня хранится в Реестре сертификатов открытых ключей в виде документа на бумажном носителе и в форме электронного документа.

#### *1.5. Приостановление действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня*

69. Приостановление действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня осуществляется:

а) по требованию уполномоченного лица центра сертификации второго уровня – владельца сертификата открытого ключа;

б) по решению уполномоченного органа;

в) по решению Центра сертификации.

70. Уполномоченное лицо центра сертификации второго уровня может потребовать приостановления действия сертификата своего открытого ключа при наличии оснований полагать, что нарушена конфиденциальность закрытого ключа, или в случае, если информация, содержащаяся в сертификате открытого ключа, не соответствует действительности.

71. Заявление на приостановление действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня (приложение № 6 к настоящему Регламенту) подается данным лицом в Центр сертификации в виде документа на бумажном носителе или в форме электронного документа.

72. В исключительных случаях, требующих незамедлительного приостановления действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня, заявление может быть подано в устной форме, с его обязательным последующим подтверждением в виде документа на бумажном носителе или в форме электронного документа в течение одного рабочего дня.

73. Заявление на приостановление действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня должно содержать:

- а) идентификационные данные уполномоченного лица центра сертификации второго уровня;
- б) серийный номер сертификата открытого ключа, действие которого приостанавливается;
- в) срок, на который приостанавливается действие сертификата открытого ключа;
- г) причину приостановления действия сертификата открытого ключа;
- д) дату подписания заявления, подписи уполномоченного лица и руководителя центра сертификации второго уровня.

74. Заявление на приостановление действия сертификата открытого ключа в виде документа на бумажном носителе подается в Центр сертификации уполномоченным лицом центра сертификации второго уровня лично, а в форме электронного документа – посредством системы электронного документооборота.

75. Заявление на приостановление действия сертификата открытого ключа в устной форме передается уполномоченным лицом центра сертификации второго уровня посредством телефонной связи.

76. Уполномоченное лицо Центра сертификации проводит аутентификацию уполномоченного лица центра сертификации второго уровня, заявившего о приостановлении действия своего сертификата открытого ключа. Аутентификация уполномоченного лица центра сертификации второго уровня выполняется по:

- а) документу, удостоверяющему личность заявителя;
- б) сертификату открытого ключа путем подтверждения подлинности заявления на приостановление действия сертификата открытого ключа в форме электронного документа;

с) ключевой фразе, сообщаемой уполномоченным лицом центра сертификации второго уровня по телефону.

77. Уполномоченное лицо Центра сертификации в течение 3 рабочих часов с момента получения заявления о приостановлении действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня принимает решение о приостановлении действия сертификата его открытого ключа.

78. Временем приостановления действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня считается время опубликования (выпуска) обновленного списка отозванных сертификатов (время, указанное в поле This Update).

79. Центр сертификации в течение 3 рабочих дней письменно уведомляет центр сертификации второго уровня о принятом решении о приостановлении действия сертификата открытого ключа или об отказе в приостановлении с указанием причин отказа.

80. Действие сертификата открытого ключа уполномоченного лица центра сертификации второго уровня приостанавливается на основании решения уполномоченного органа, оформленного в виде распоряжения директора Службы информации и безопасности.

81. Если Центр сертификации имеет основания полагать, что нарушена конфиденциальность закрытого ключа уполномоченного лица центра сертификации второго уровня или информация, содержащаяся в его сертификате открытого ключа, не соответствует действительности, Центр сертификации вправе принять в одностороннем порядке решение о приостановлении действия соответствующего сертификата открытого ключа.

82. В случае приостановления действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня на основании решения уполномоченного органа или Центра сертификации Центр сертификации незамедлительно, по средствам телефонной связи, уведомляет центр сертификации второго уровня о приостановлении действия сертификата открытого ключа его уполномоченного лица, с последующим письменным уведомлением в течение 3 рабочих дней.

83. Действие сертификата открытого ключа уполномоченного лица центра сертификации второго уровня приостанавливается на срок до 30 дней.

84. Сертификат открытого ключа уполномоченного лица центра сертификации второго уровня, действие которого приостановлено, помещается в течение 3 рабочих часов в список отозванных сертификатов, а Центром сертификации выпускается обновленный список отозванных сертификатов.

85. В случае, если до истечения срока, на который было приостановлено действие сертификата открытого ключа, не принимается решение о возобновлении его действия, сертификат открытого ключа отзывается.

86. Возобновление действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня осуществляется:

а) по требованию уполномоченного лица центра сертификации второго уровня – владельца сертификата открытого ключа;

- b) по решению уполномоченного органа;
- c) по решению Центра сертификации.

87. Заявление на возобновление действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня (приложение № 7 к настоящему Регламенту) представляет собой документ на бумажном носителе, заверенный собственноручными подписями уполномоченного лица и руководителя центра сертификации второго уровня.

88. Заявление на возобновление действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня подается в Центр сертификации лично уполномоченным лицом центра сертификации второго уровня не позднее, чем за 5 рабочих дней до окончания срока, на который было приостановлено действие сертификата открытого ключа.

89. Заявление на возобновление действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня должно содержать:

- a) идентификационные данные уполномоченного лица центра сертификации второго уровня;
- b) серийный номер сертификата открытого ключа, действие которого приостановлено;
- c) срок, на который было приостановлено действие сертификата открытого ключа;
- d) причину приостановления действия сертификата открытого ключа;
- e) основания для возобновления действия сертификата открытого ключа;
- f) дату подписания заявления, подписи уполномоченного лица и руководителя центра сертификации второго уровня.

90. Уполномоченное лицо Центра сертификации в течение 5 рабочих дней с даты получения заявления о возобновлении действия сертификата открытого ключа принимает решение о возобновлении действия сертификата.

91. Центр сертификации в течение 3 рабочих дней письменно уведомляет центр сертификации второго уровня о принятом решении о возобновлении действия сертификата открытого ключа или об отказе в возобновлении, с указанием причин отказа.

92. Действие сертификата открытого ключа уполномоченного лица центра сертификации второго уровня, приостановленного на основании решения уполномоченного органа, возобновляется на основании решения уполномоченного органа, оформленного в виде распоряжения директора Службы информации и безопасности.

93. В случае если действие сертификата открытого ключа центра сертификации второго уровня было приостановлено по решению Центра сертификации, Центр сертификации вправе принять в одностороннем порядке решение о возобновлении действия соответствующего сертификата открытого ключа.

94. В случае возобновления действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня на основании решения уполномоченного органа или Центра сертификации Центр

сертификации в течение 3 рабочих дней направляет центру сертификации второго уровня письменное уведомление о возобновлении действия сертификата.

95. Сертификат открытого ключа уполномоченного лица центра сертификации второго уровня, действие которого было возобновлено, в течение 3 рабочих часов исключается из списка отозванных сертификатов, а Центр сертификации выпускает обновленный список отозванных сертификатов.

96. Временем возобновления действия сертификата открытого ключа уполномоченного лица центра сертификации второго уровня считается время опубликования (выпуска) обновленного списка отозванных сертификатов (время, указанное в поле This Update).

#### *1.6. Отзыв сертификата открытого ключа уполномоченного лица центра сертификации второго уровня*

97. Сертификат открытого ключа уполномоченного лица центра сертификации второго уровня отзывается:

- a) по требованию уполномоченного лица центра сертификации второго уровня – владельца сертификата открытого ключа;
- b) по решению уполномоченного органа;
- c) в случае установленного факта компрометации закрытого ключа;
- d) при обнаружении несоответствия действительности сведений, указанных в заявке на сертификацию открытого ключа или в сертификате открытого ключа;
- e) при внесении изменений в сертификат открытого ключа;
- f) по истечении срока, на который было приостановлено действие сертификата открытого ключа, если не было принято решение о возобновлении действия сертификата;
- g) по истечении срока действия сертификата открытого ключа.

98. Уполномоченное лицо центра сертификации второго уровня может потребовать отзыва своего сертификата открытого ключа при установлении фактов нарушения конфиденциальности своего закрытого ключа или недействительности информации, содержащейся в сертификате, а также в других случаях, предусмотренных Регламентом центра сертификации второго уровня.

99. Заявление на отзыв сертификата открытого ключа уполномоченного лица центра сертификации второго уровня (приложение № 8 к настоящему Регламенту) представляет собой документ на бумажном носителе, заверенный собственноручными подписями уполномоченного лица и руководителя центра сертификации второго уровня.

100. Заявление на отзыв сертификата открытого ключа уполномоченного лица центра сертификации второго уровня подается в Центр сертификации лично уполномоченным лицом центра сертификации второго уровня.

101. Заявление на отзыв сертификата открытого ключа уполномоченного лица центра сертификации второго уровня должно содержать:

- a) идентификационные данные уполномоченного лица центра сертификации второго уровня;
- b) серийный номер сертификата открытого ключа, который подлежит отзыву;
- c) причину отзыва сертификата открытого ключа;
- d) дату подписания заявления, подписи уполномоченного лица и руководителя центра сертификации второго уровня.

102. Уполномоченное лицо Центра сертификации в течение 3 рабочих часов с момента получения заявления об отзыве сертификата открытого ключа уполномоченного лица центра сертификации второго уровня принимает решение об отзыве сертификата.

103. Центр сертификации в течение 3 рабочих дней письменно уведомляет центр сертификации второго уровня о принятом решении об отзыве сертификата открытого ключа или об отказе в отзыве сертификата с указанием причин отказа.

104. Сертификат открытого ключа уполномоченного лица центра сертификации второго уровня отзывается на основании решения уполномоченного органа, оформленного в виде распоряжения директора Службы информации и безопасности.

105. Центр сертификации вправе принять в одностороннем порядке решение об отзыве сертификата открытого ключа уполномоченного лица центра сертификации второго уровня:

- a) в случае установленного факта компрометации закрытого ключа;
- b) при обнаружении несоответствия действительности сведений, указанных в заявке на сертификацию открытого ключа или в сертификате открытого ключа;
- c) при внесении изменений в сертификат открытого ключа;
- d) по истечении срока, на который было приостановлено действие сертификата открытого ключа, если не было принято решение о возобновлении действия сертификата;
- e) по истечении срока действия сертификата открытого ключа.

106. В случае отзыва сертификата открытого ключа уполномоченного лица центра сертификации второго уровня на основании решения уполномоченного органа или Центра сертификации Центр сертификации незамедлительно, по средствам телефонной связи, уведомляет центр сертификации второго уровня об отзыве сертификата открытого ключа его уполномоченного лица с последующим письменным уведомлением в течение 3 рабочих дней.

107. Отозванный сертификат открытого ключа уполномоченного лица центра сертификации второго уровня в течение 3 рабочих часов вносится в список отозванных сертификатов, а Центр сертификации выпускает обновленный список отозванных сертификатов.

108. Временем отзыва сертификата открытого ключа уполномоченного лица центра сертификации второго уровня считается время опубликования (выпуска) обновленного списка отозванных сертификатов (время, указанное в поле This Update).

109. При отзыве сертификата открытого ключа по причине истечения срока его действия данный сертификат в список отозванных сертификатов не вносится.

110. В случае увольнения уполномоченного лица центра сертификации второго уровня его закрытый ключ уничтожается в соответствии с требованиями, установленными уполномоченным органом, а сертификат соответствующего открытого ключа продолжает действовать до истечения срока его действия.

### *1.7. Подтверждение подлинности и действительности сертификата открытого ключа*

111. Центр сертификации подтверждает подлинность и действительность сертификатов открытых ключей:

а) уполномоченных лиц центров сертификации второго уровня – по заявлениям пользователей цифровой подписи;

б) выданных центрами сертификации второго уровня – по запросам судебной инстанции, лиц или органов, имеющих такое право в силу закона, а также в других случаях, предусмотренных законодательством в сфере применения цифровой подписи.

112. Центр сертификации обеспечивает пользователям цифровой подписи возможность самостоятельно определять подлинность и действительность сертификата открытого ключа уполномоченного лица центра сертификации второго уровня путем:

предоставления свободного доступа к электронным документам, содержащимся в Реестре сертификатов открытых ключей;

свободного распространения и опубликования списка отозванных сертификатов в форме электронного документа.

113. Заявление пользователя цифровой подписи на подтверждение подлинности и действительности сертификата открытого ключа представляет собой документ на бумажном носителе, заверенный собственноручной подписью заявителя (приложение № 9 к настоящему Регламенту).

114. Заявление подается в Центр сертификации вместе с материальным носителем, содержащим сертификат открытого ключа в форме электронного документа, подлинность и действительность которого должна быть подтверждена.

115. В течение 3 рабочих дней Центр сертификации представляет заявителю заключение по результатам проверки подлинности и действительности сертификата открытого ключа, содержащее:

а) время и место проведения проверки;

б) основания для проведения проверки;

- с) сведения о сотруднике Центра сертификации, проводившем проверку (фамилия, имя, занимаемая должность);
- d) содержание и результаты проверки;
- е) оценку результатов проверки и соответствующие выводы;
- f) другие данные, установленные Центром сертификации.

116. Центр сертификации может отказать заявителю в проверке подлинности и действительности сертификата открытого ключа уполномоченного лица центра сертификации второго уровня, если не были предъявлены все необходимые электронные документы или поврежден материальный носитель.

## ***Раздел 2. Управление закрытым и открытым ключами уполномоченного лица Центра сертификации***

117. Срок действия закрытого ключа уполномоченного лица Центра сертификации – 2,5 года. Начало периода действия закрытого ключа исчисляется с даты и времени начала срока действия соответствующего сертификата открытого ключа.

118. Срок действия сертификата открытого ключа, соответствующего закрытому ключу уполномоченного лица Центра сертификации, – 5 лет.

119. По истечении срока действия закрытого ключа уполномоченного лица Центра сертификации закрытый ключ уничтожается, создаются новые закрытый и открытый ключи, а также сертификат открытого ключа.

120. Плановая смена закрытого ключа и соответствующего ему открытого ключа уполномоченного лица Центра сертификации выполняется не ранее чем через 2 года и 5 месяцев и не позднее чем через 2 года и 6 месяцев после начала срока действия закрытого ключа уполномоченного лица Центра сертификации.

121. Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации закрытого ключа уполномоченного лица Центра сертификации.

122. Процедуры смены ключей осуществляются в соответствии с требованиями, установленными уполномоченным органом.

123. Закрытый ключ уполномоченного лица Центра сертификации используется исключительно с целью подписания цифровой подписью:

- а) сертификата открытого ключа уполномоченного лица Центра сертификации;
- б) сертификатов открытых ключей уполномоченных лиц центров сертификации второго уровня;
- с) списков отозванных сертификатов.

124. Закрытый ключ уполномоченного лица Центра сертификации хранится и используется в условиях, исключающих нарушение его конфиденциальности.

125. Доступ к материальному носителю закрытого ключа уполномоченного лица Центра сертификации осуществляется по письменному

разрешению руководителя Центра сертификации, при непосредственном присутствии уполномоченного лица Центра сертификации (администратора сертификации), администратора безопасности Центра сертификации и руководителя Центра сертификации таким образом, чтобы при отсутствии хотя бы одного из этих лиц, доступ к ключу был неосуществим. В случае временного отсутствия администратора безопасности и руководителя Центра сертификации доступ осуществляется в присутствии замещающих их лиц.

126. Уполномоченное лицо Центра сертификации использует свой закрытый ключ в присутствии администратора безопасности без нарушения конфиденциальности закрытого ключа.

127. Руководитель Центра сертификации несет ответственность за организацию безопасного доступа к материальному носителю закрытого ключа и санкционированного использования ключа.

128. Руководитель центра сертификации, уполномоченное лицо Центра сертификации (администратор сертификации) и администратор безопасности несут персональную ответственность за безопасное использование уполномоченным лицом своего закрытого ключа.

### ***Раздел 3. Информационные ресурсы Центра сертификации***

129. Основным информационным ресурсом Центра сертификации является Реестр сертификатов открытых ключей.

130. Реестр сертификатов открытых ключей представляет собой набор документов на бумажном носителе и электронных документов, включающий:

- a) сертификаты открытых ключей уполномоченных лиц Центра сертификации;
- b) решения о приостановлении действия, возобновлении действия и отзыве сертификатов открытых ключей уполномоченных лиц Центра сертификации;
- c) заявки на сертификацию открытых ключей уполномоченных лиц центров сертификации второго уровня;
- d) сертификаты открытых ключей уполномоченных лиц центров сертификации второго уровня;
- e) заявления на приостановление действия, возобновление действия и отзыв сертификатов открытых ключей уполномоченных лиц центров сертификации второго уровня;
- f) списки отозванных сертификатов.

131. Архивному хранению подлежат следующие информационные ресурсы Центра сертификации:

- a) Реестр сертификатов открытых ключей;
- b) журналы аудита программно-технического комплекса Центра сертификации;
- c) служебные документы Центра сертификации согласно критериям, установленным руководителем Центра.

132. Срок хранения архивных документов Центра сертификации – 20 лет.

133. Подготовка к уничтожению и уничтожение архивных документов осуществляется комиссией, формируемой из числа сотрудников Центра сертификации и уполномоченного органа.

134. Подготовка к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками Центра сертификации, назначенными руководителем Центра.

135. Защита информационных ресурсов Центра сертификации осуществляется в соответствии с действующим законодательством и требованиями, установленными уполномоченным органом.

136. Порядок осуществления доступа к информационным ресурсам Центра сертификации, включая доступ к архивным документам, регламентируется действующим законодательством, требованиями уполномоченного органа и настоящим Регламентом.

137. Доступ пользователей цифровой подписи к Реестру сертификатов открытых ключей осуществляется посредством:

а) официального электронного информационного ресурса Центра сертификации по адресу: [www.pki.sis.md](http://www.pki.sis.md);

б) электронной почты: [pki@sis.md](mailto:pki@sis.md);

в) письменного запроса пользователя цифровой подписи в соответствии с процедурой, установленной настоящим Регламентом. Почтовый адрес: MD-2004, Республика Молдова, мун. Кишинэу, бул. Штефан чел Маре ши Сфынт, 166, Центр сертификации открытых ключей высшего уровня.

138. Центр сертификации публикует на страницах своего официального электронного информационного ресурса:

а) обновленный список отозванных сертификатов в форме электронного документа;

б) электронные копии сертификатов открытых ключей на бумажном носителе уполномоченных лиц Центра сертификации и уполномоченных лиц центров сертификации второго уровня в формате PDF;

в) сертификаты открытых ключей уполномоченных лиц Центра сертификации и уполномоченных лиц центров сертификации второго уровня в форме электронных документов.

139. Центр сертификации осуществляет автоматическую рассылку обновленного списка отозванных сертификатов центрам сертификации второго уровня посредством электронной почты.

#### ***Раздел 4. Средства обеспечения деятельности Центра сертификации***

140. Центр сертификации создает и эксплуатирует программно-технический комплекс, состоящий из следующих компонентов:

а) служба сертификации;

б) служба регистрации;

в) служба реестра;

d) служба эталонной проверки цифровой подписи.

141. Служба сертификации является базовым технологическим компонентом программно-технического комплекса Центра сертификации, обеспечивающим:

a) создание сертификата открытого ключа уполномоченного лица Центра сертификации в форме электронного документа;

b) создание сертификата открытого ключа уполномоченного лица центра сертификации второго уровня в форме электронного документа;

c) создание списка отозванных сертификатов.

142. Ответственность за эксплуатацию службы сертификации возлагается на уполномоченное лицо Центра сертификации (администратора сертификации) и на системного администратора.

143. Служба регистрации является технологическим компонентом программно-технического Центра сертификации, обеспечивающим регистрацию уполномоченных лиц центров сертификации второго уровня.

144. Ответственность за эксплуатацию службы регистрации возлагается на администратора регистрации.

145. Служба реестра является технологическим компонентом программно-технического комплекса Центра сертификации, обеспечивающим:

a) хранение сертификатов открытых ключей уполномоченных лиц Центра сертификации;

b) хранение сертификатов открытых ключей уполномоченных лиц центров сертификации второго уровня;

c) хранение заявок на сертификацию открытых ключей;

d) хранение регистрационной информации уполномоченных лиц центров сертификации второго уровня;

e) публикацию и распространение списков отозванных сертификатов;

f) доступ к действительным сертификатам открытых ключей, а также к спискам отозванных сертификатов;

g) хранение другой служебной информации Центра сертификации.

146. Служба эталонной проверки цифровой подписи является технологическим компонентом программно-технического комплекса Центра сертификации, обеспечивающим подтверждение подлинности сертификатов открытых ключей и других электронных документов.

147. Технические средства обеспечения работы программно-технического комплекса Центра сертификации включают:

a) серверное оборудование;

b) телекоммуникационное оборудование;

c) компьютеризированные рабочие места администраторов Центра сертификации;

d) устройства печати на бумажных носителях;

e) другое вспомогательное оборудование.

148. Ответственность за эксплуатацию технических средств обеспечения работы программно-технического комплекса Центра сертификации возлагается на системного администратора.

149. В составе компонентов программно-технического комплекса Центра сертификации функционируют криптографические средства защиты информации, включая:

- a) средства цифровой подписи;
- b) программно-технические комплексы защиты от несанкционированного доступа и обеспечения целостности программно-аппаратных средств.

150. Ответственность за эксплуатацию средств защиты информации возлагается на системного администратора и администратора безопасности.

151. Программно-технический комплекс должен соответствовать требованиям, установленным уполномоченным органом, и технологическим характеристикам, указанным в приложении № 10 к настоящему Регламенту.

#### **IV. Обеспечение безопасности и защита конфиденциальной информации**

##### ***Раздел 1. Конфиденциальность информации***

152. Информация, обрабатываемая и хранящаяся в Центре сертификации, охраняется законом.

153. Информация, хранящаяся в журналах аудита Центра сертификации, считается конфиденциальной.

154. Не являются конфиденциальной информацией данные, содержащиеся:

- a) в сертификатах открытых ключей уполномоченных лиц центров сертификации второго уровня;
- b) в списках отозванных сертификатов.

155. Центр сертификации обеспечивает сохранность и контроль доступа к охраняемой законом информации в соответствии с законодательством Республики Молдова.

##### ***Раздел 2. Инженерно-технические меры защиты информации***

156. Инженерно-технические меры защиты информации должны обеспечивать возможность непрерывного функционирования в течение продолжительного времени программно-технического комплекса Центра сертификации.

157. Серверы службы сертификации, службы регистрации и службы реестра размещаются в серверных помещениях, в серверных стойках.

158. Серверные помещения Центра сертификации оборудуются системой контроля доступа.

159. Доступ в серверные помещения Центра сертификации осуществляется в соответствии с требованиями, установленными уполномоченным органом.

160. Остальные технические средства программно-технического комплекса Центра сертификации размещаются в рабочих помещениях Центра.

161. Серверные и рабочие помещения оборудуются средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима.

162. Противопожарная безопасность помещений Центра сертификации обеспечивается в соответствии с нормами и требованиями, предусмотренными действующим законодательством.

163. Технические средства Центра сертификации должны быть подключены к сети гарантированного электропитания.

### ***Раздел 3. Программно-аппаратные меры защиты информации***

164. Программно-технический комплекс Центра сертификации должен обеспечивать контроль целостности программных и технических средств.

165. Ответственность за выполнение мероприятий по контролю целостности программных и технических средств программно-технического комплекса Центра сертификации возложена на системного администратора и администратора безопасности.

166. Средства программно-технического комплекса Центра сертификации должны обеспечивать резервное копирование критически важной информации по мере необходимости.

167. При доступе к процедурам Центра сертификации используется функциональное разграничение членов группы администраторов, обслуживающих программно-технический комплекс Центра сертификации.

168. Серверы службы сертификации, службы регистрации и службы реестра, а также рабочие места администраторов Центра сертификации оснащаются программно-аппаратными средствами защиты от несанкционированного доступа.

169. Доступ инженерного состава и системных администраторов к серверам службы сертификации, службы регистрации и службы реестра для выполнения регламентных работ осуществляется в присутствии администраторов, отвечающих за эксплуатацию соответствующего прикладного программного обеспечения.

170. Организация доступа к техническим средствам программно-технического комплекса Центра сертификации, размещенных в рабочих помещениях, возлагается на администраторов Центра сертификации, ответственных за эксплуатацию данных технических средств.

### ***Раздел 4. Организационные меры защиты информации***

171. Организационные меры защиты информации должны обеспечивать:

- a) сохранность документов и материальных ценностей;
- b) обнаружение и задержание нарушителей, пытающихся проникнуть в здание (помещения) Центра сертификации.

172. В Центре сертификации предусмотрены следующие должности:

а) администратор регистрации, в основные обязанности которого входит: регистрация и учет уполномоченных лиц центров сертификации второго уровня, подготовка запросов на создание сертификатов открытых ключей, выдача сертификатов открытых ключей уполномоченным лицам центров сертификации второго уровня;

б) администратор сертификации (уполномоченное лицо Центра сертификации), в основные обязанности которого входит: создание, приостановление, возобновление действия и отзыв сертификатов открытых ключей, создание и опубликование (выпуск) списка отозванных сертификатов;

с) администратор безопасности, в основные обязанности которого входит: контроль безопасности всех процедур и механизмов Центра сертификации, обеспечение безопасности компонентов программно-технического комплекса Центра сертификации;

д) системный администратор, в основные обязанности которого входит: установка, конфигурация и поддержка функционирования службы сертификации, службы регистрации и службы реестра.

173. Уполномоченное лицо Центра сертификации назначается приказом директора Службы информации и безопасности по предложению руководителя Центра сертификации. Требования к квалификации и должностные обязанности уполномоченного лица Центра сертификации определяются должностной инструкцией.

174. Системный администратор и администратор безопасности Центра сертификации должны иметь высшее инженерно-техническое образование.

175. Доступ сотрудников к документам Центра сертификации организуется в соответствии с должностными обязанностями, утвержденными руководителем Центра сертификации.

## **V. Взаимодействие уполномоченных лиц центров сертификации второго уровня и пользователей цифровой подписи с Центром сертификации**

### ***Раздел 1. Порядок взаимодействия уполномоченных лиц центров сертификации второго уровня и пользователей цифровой подписи с Центром сертификации***

176. Взаимодействие центров сертификации второго уровня и пользователей цифровой подписи с Центром сертификации осуществляется в соответствии с процедурами, установленными настоящим Регламентом, и требованиями в сфере цифровой подписи.

177. Центр сертификации обеспечивает доступ центров сертификации второго уровня и пользователей цифровой подписи к Реестру сертификатов открытых ключей в соответствии с настоящим Регламентом.

178. Центр сертификации публикует обновленный список отозванных сертификатов и осуществляет его автоматическую рассылку центрам сертификации второго уровня.

179. В целях взаимодействия уполномоченное лицо Центра сертификации предоставляет уполномоченным лицам центров сертификации второго уровня свои контактные данные (номер телефона, факс, почтовый адрес, адрес электронной почты).

180. В случае отзыва сертификата открытого ключа уполномоченного лица Центра сертификации одновременно отзываются и сертификаты открытых ключей уполномоченных лиц центров сертификации второго уровня.

181. Пользователи цифровой подписи используют сертификат открытого ключа уполномоченного лица Центра сертификации в процессе проверки подлинности цифровой подписи в электронном документе.

182. В процессе взаимодействия уполномоченных лиц центров сертификации второго уровня и пользователей цифровой подписи с Центром сертификации могут возникнуть спорные ситуации. В соответствии с настоящим Регламентом подлежат разрешению спорные ситуации, возникшие в связи с:

а) оспариванием уполномоченным лицом центра сертификации второго уровня или пользователем цифровой подписи действительности и подлинности сертификата открытого ключа уполномоченного лица Центра сертификации;

б) оспариванием пользователем цифровой подписи действительности и подлинности сертификата открытого ключа уполномоченного лица центра сертификации второго уровня;

в) оспариванием полномочий уполномоченного лица Центра сертификации;

г) оспариванием полномочий уполномоченного лица центра сертификации второго уровня;

д) оспариванием сферы применения цифровой подписи и иных ограничений, указанных в сертификатах открытых ключей, выданных Центром сертификации;

е) недоверием к средствам цифровой подписи, применяемым Центром сертификации;

ж) в других случаях возникновения спорных ситуаций в связи с применением цифровой подписи.

183. Спорная ситуация разрешается в рабочем порядке заинтересованными сторонами в соответствии с Регламентом о разрешении спорных ситуаций в сфере применения цифровой подписи, утвержденным уполномоченным органом.

184. В случае, если спорная ситуация признается сторонами разрешенной, оформляется акт об урегулировании спорной ситуации, который подписывается сторонами.

185. В случае невозможности разрешения спорной ситуации в рабочем порядке стороны могут обратиться в судебную инстанцию в порядке, предусмотренном законодательством.

***Раздел 2. Права и обязанности уполномоченного лица  
центра сертификации второго уровня при взаимодействии  
с Центром сертификации***

186. При взаимодействии с Центром сертификации уполномоченное лицо центра сертификации второго уровня имеет право:

- a) создавать свои открытый и закрытый ключи с использованием сертифицированных средств цифровой подписи;
- b) подавать заявку на сертификацию своего открытого ключа;
- c) подавать заявления на отзыв, приостановление или возобновление действия сертификата открытого ключа в течение срока действия соответствующего закрытого ключа;
- d) получать доступ к Реестру сертификатов открытых ключей;
- e) применять сертификат открытого ключа уполномоченного лица Центра сертификации для проверки подлинности цифровой подписи в сертификатах открытых ключей, выданных Центром сертификации;
- f) получать список отозванных сертификатов Центра сертификации;
- g) применять список отозванных сертификатов Центра сертификации для определения действительности сертификата открытого ключа уполномоченного лица Центра сертификации;
- h) получать копию сертификата открытого ключа уполномоченного лица Центра сертификации на бумажном носителе;
- i) обращаться в Центр сертификации за подтверждением подлинности и действительности выданного им сертификата открытого ключа уполномоченного лица центра сертификации второго уровня;
- j) получать методическую помощь от уполномоченного лица Центра сертификации.

187. При взаимодействии с Центром сертификации уполномоченное лицо центра сертификации второго уровня обязано:

- a) выполнять требования законодательства в сфере применения цифровой подписи;
- b) представлять информацию в объеме, определенном настоящим Регламентом;
- c) исключить доступ другого лица к своему закрытому ключу, принимать меры по предотвращению компрометации закрытого ключа;
- d) применять свой закрытый ключ в соответствии со сферами применения цифровой подписи и иными ограничениями, указанными в сертификате открытого ключа;
- e) немедленно сообщать Центру сертификации о компрометации своего закрытого ключа;
- f) не использовать свой закрытый ключ при наличии оснований (подозрений) полагать, что нарушена конфиденциальность закрытого ключа;
- g) не использовать свой закрытый ключ в период рассмотрения заявки на сертификацию соответствующего ему открытого ключа, заявлений на отзыв,

приостановление или возобновление действия сертификата соответствующего открытого ключа;

h) не использовать свой закрытый ключ, если сертификат соответствующего открытого ключа приостановлен или отозван.

### ***Раздел 3. Права пользователя цифровой подписи при взаимодействии с Центром сертификации***

188. При взаимодействии с Центром сертификации пользователь цифровой подписи имеет право:

a) создавать свои открытый и закрытый ключи с использованием сертифицированных средств цифровой подписи;

b) получать список отозванных сертификатов Центра сертификации;

c) получать доступ к Реестру сертификатов открытых ключей;

d) применять список отозванных сертификатов Центра сертификации для проверки действительности сертификатов открытых ключей уполномоченных лиц Центра сертификации и центров сертификации второго уровня;

e) применять сертификат открытого ключа уполномоченного лица Центра сертификации для подтверждения подлинности сертификата открытого ключа уполномоченного лица центра сертификации второго уровня;

f) обращаться в Центр сертификации за подтверждением подлинности и действительности сертификатов открытых ключей уполномоченного лица Центра сертификации и уполномоченных лиц центра сертификации второго уровня.

## **VI. Реорганизация и ликвидация Центра сертификации**

189. Реорганизация и ликвидация Центра сертификации осуществляется в соответствии с законодательством.

190. При реорганизации Центра сертификации и передаче его функций другому учреждению совместным решением руководителей заинтересованных учреждений создается комиссия по передаче Центра сертификации.

191. В состав комиссии по передаче Центра сертификации должны входить:

a) представители сторон;

b) руководитель Центра сертификации или замещающее его лицо;

c) представитель уполномоченного органа;

d) другие лица, назначаемые сторонами.

192. По окончании работы комиссия составляет акт приема-передачи, в соответствии с которым новому учреждению передается Реестр сертификатов открытых ключей, а также права и обязанности Центра сертификации. Акт подписывается всеми членами комиссии и утверждается руководителями заинтересованных учреждений.

193. Реестр сертификатов открытых ключей в форме электронных документов передается на материальных носителях, а Реестр сертификатов открытых ключей на бумажных носителях передается в виде архива документов на бумажных носителях.

194. При передаче Центра сертификации закрытые ключи уполномоченных лиц Центра сертификации уничтожаются без нарушения их конфиденциальности в соответствии с требованиями, установленными уполномоченным органом, а сертификаты соответствующих открытых ключей, переданные другому центру сертификации, продолжают действовать до истечения срока действия.

195. При ликвидации Центра сертификации приказом директора Службы информации и безопасности создается ликвидационная комиссия, в задачи которой входит проведение процедуры ликвидации в соответствии с действующим законодательством и требованиями, установленными уполномоченным органом.

196. В состав ликвидационной комиссии должны входить:

- a) руководитель Центра сертификации или замещающее его лицо;
- b) представитель уполномоченного органа;
- c) другие лица, назначенные приказом.

197. По окончании работы ликвидационная комиссия составляет акт о ликвидации, в соответствии с которым Центр сертификации прекращает свою деятельность, а Реестр сертификатов открытых ключей передается уполномоченному органу и подлежит архивному хранению в соответствии с законодательством.

198. Реестр сертификатов открытых ключей ликвидированного Центра сертификации в форме электронных документов передается в уполномоченный орган на материальных носителях, а Реестр сертификатов открытых ключей на бумажных носителях передается в виде архива документов на бумажных носителях, о чем составляется акт приема-передачи. Акт подписывается руководителем Центра сертификации, представителем уполномоченного органа, ответственным за хранение, и утверждается директором Службы информации и безопасности.

199. При ликвидации Центра сертификации закрытые ключи уполномоченных лиц Центра сертификации уничтожаются без нарушения их конфиденциальности, а сертификаты соответствующих открытых ключей отзываются.

Приложение № 1  
к Регламенту Центра сертификации  
открытых ключей высшего уровня

**Структура сертификата открытого ключа  
уполномоченного лица Центра сертификации высшего уровня**

Сертификат открытого ключа уполномоченного лица Центра сертификации высшего уровня содержит следующие поля:

Наименование (на англ. языке)	Описание	Содержание
<i>Базовые поля</i>		
Version	Версия	V3
Serial Number	Регистрационный номер сертификата	Номер
Issuer	Идентификационные данные Центра сертификации высшего уровня	N = Фамилия, имя уполномоченного лица Центра сертификации высшего уровня, IDNP CN = MoldovaCA L = Кишинэу S = Республика Молдова OU = Центр сертификации высшего уровня O = Служба информации и безопасности Республики Молдова, IDNO P = Телефон уполномоченного лица T = Должность уполномоченного лица Центра сертификации высшего уровня C = MD E = pki@sis.md
Validity Period	Срок действия сертификата	Действителен с: " __ " ____ 20__ г. чч:мм:сс GMT Действителен по: " __ " ____ 20__ г. чч:мм:сс GMT

Subject	Идентификационные данные Центра сертификации высшего уровня	<p>N = Фамилия, имя уполномоченного лица Центра сертификации высшего уровня, IDNP</p> <p>CN = MoldovaCA</p> <p>L = Кишинэу</p> <p>S = Республика Молдова</p> <p>OU = Центр сертификации высшего уровня</p> <p>O = Служба информации и безопасности Республики Молдова, IDNO</p> <p>R = Телефон уполномоченного лица</p> <p>T = Должность уполномоченного лица Центра сертификации высшего уровня</p> <p>C = MD</p> <p>E = pki@sis.md</p>
FriendlyName	Понятное имя	MoldovaCA
Public Key	Открытый ключ	Открытый ключ (алгоритм RSA)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	SHA-1/RSA
Issuer Sign	Цифровая подпись издателя сертификата	Подпись издателя в соответствии с SHA-1/RSA
<i>Дополнительные поля</i>		
Key Usage	Использование ключа	Неотрекаемость, Цифровая подпись в сертификатах уполномоченных лиц центров сертификации второго уровня, Цифровая подпись в списке отозванных сертификатов (CRL)
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа уполномоченного лица Центра сертификации высшего уровня, соответствующего данному сертификату

PrivateKeyUsagePeriod	Период действия закрытого ключа	Действителен с: " __ " ____ 20__ г. чч:мм:сс GMT Действителен по: " __ " ____ 20__ г. чч:мм:сс GMT
CRL Distribution Point	Точка распределения списка отозванных сертификатов (CRL)	URL= <a href="http://www.pki.sis.md/cert/rootca.crl">http://www.pki.sis.md/cert/rootca.crl</a>
Certificate Template	Шаблон сертификата	СА

### Структура списка отозванных сертификатов (CRL)

Список отозванных сертификатов Центра сертификации высшего уровня содержит следующие поля:

Наименование (на англ. языке)	Описание	Содержание
<i>Базовые поля</i>		
Version	Версия	V2
Issuer	Издатель CRL	<p>N = Фамилия, имя уполномоченного лица Центра сертификации высшего уровня, IDNP</p> <p>CN = MoldovaCA</p> <p>L = Кишинэу</p> <p>S = Республика Молдова</p> <p>OU = Центр сертификации высшего уровня</p> <p>O = Служба информации и безопасности Республики Молдова, IDNO</p> <p>P = Телефон уполномоченного лица</p> <p>T = Должность уполномоченного лица Центра сертификации высшего уровня</p> <p>C = MD</p> <p>E = pki@sis.md</p>
thisUpdate	Время издания CRL	"__" ____ 20__ г. чч:мм:сс GMT
nextUpdate	Время, по которое действителен CRL	"__" ____ 20__ г. чч:мм:сс GMT
RevokedCertificates	Список отозванных сертификатов	<p>Серийный номер сертификата (CertificateSerialNumber)</p> <p>Время отзыва или приостановления действия сертификата (Time)</p>

Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	SHA-1/RSA
Issuer Sign	Цифровая подпись издателя сертификата	Подпись издателя в соответствии с SHA-1/RSA
<i><b>Дополнительные поля</b></i>		
Reason Code	Код причины отзыва сертификата	"0" Не указана "1" Компрометация закрытого ключа "2" Компрометация Центра сертификации "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановление действия
holdInstructionCode	Код причины временного приостановления сертификата	Код причины временного приостановления сертификата (OID)
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа уполномоченного лица Центра сертификации высшего уровня, с использованием которого подписан CRL
CRLNumber	Серийный номер	Серийный номер CRL

Приложение № 3  
к Регламенту Центра сертификации  
открытых ключей высшего уровня

**Образец заявки на сертификацию открытого ключа уполномоченного лица  
центра сертификации второго уровня**

**Центру сертификации открытых  
ключей высшего уровня**

**Заявление  
на сертификацию открытого ключа**

Настоящим, \_\_\_\_\_,  
(фамилия и имя уполномоченного лица)

Номер документа, удостоверяющего личность: \_\_\_\_\_  
IDNP: \_\_\_\_\_, e-mail: \_\_\_\_\_,  
почтовый адрес: \_\_\_\_\_  
телефон/факс: \_\_\_\_\_,  
являясь уполномоченным лицом \_\_\_\_\_  
\_\_\_\_\_  
(наименование центра сертификации второго уровня)

свидетельство о регистрации № \_\_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 200\_\_ г.,  
выданное \_\_\_\_\_  
(наименование юридического лица, создавшего центр сертификации второго уровня)  
\_\_\_\_\_  
(юридический адрес)

Прошу создать и выдать сертификат открытого ключа

\_\_\_\_\_,  
в соответствии с указанными в настоящем заявлении данными и внести в сертификат  
следующую информацию:

N (Name) = \_\_\_\_\_  
(фамилия, имя уполномоченного лица)

IDNP = \_\_\_\_\_  
(идентификационный номер физического лица – уполномоченного лица)

CN (Common Name) = \_\_\_\_\_  
(наименование центра сертификации)

L (Locality) = \_\_\_\_\_  
(населенный пункт)

S (State) = \_\_\_\_\_  
(государство)

OU (Organizational Unit) = \_\_\_\_\_  
(наименование подразделения юридического лица)

O (Organization) = \_\_\_\_\_  
(наименование юридического лица)

T (Title) = \_\_\_\_\_  
(должность уполномоченного лица)

C (Country) = \_\_\_\_\_  
(код государства)

E (Email) = \_\_\_\_\_  
(адрес электронной почты)

Шаблоны сертификата:

- \_\_\_\_\_;
- \_\_\_\_\_.

Средство цифровой подписи (CryptoProvider): \_\_\_\_\_

Сертифицируемый открытый ключ: \_\_\_\_\_

Имя файла запроса на сертификацию открытого ключа в соответствии с PKCS#10 \_\_\_\_\_

Почтовый код и адрес юридического лица \_\_\_\_\_

Контактный телефон юридического лица \_\_\_\_\_

Контактный телефон уполномоченного лица \_\_\_\_\_,  
включая следующие данные о сферах применения цифровой подписи и иные установленные  
ограничения: \_\_\_\_\_

Должностные обязанности \_\_\_\_\_  
(должность, фамилия, имя)

подтверждены \_\_\_\_\_  
(реквизиты документа о назначении уполномоченного лица)

\_\_\_\_\_ 200\_\_ г.  
Должность \_\_\_\_\_  
\_\_\_\_\_ / \_\_\_\_\_  
(подпись) (фамилия, имя)  
м.п.

Настоящим подтверждаю, что заявка на сертификацию открытого ключа на имя \_\_\_\_\_  
(фамилия и имя)

личность \_\_\_\_\_  
(фамилия и имя)

идентифицирована. Сведения, указанные в заявке, проверены.

\_\_\_\_\_ 200\_\_ г.  
Администратор регистрации  
\_\_\_\_\_ / \_\_\_\_\_  
(подпись) (фамилия, имя)  
м.п.

Приложение № 4  
к Регламенту Центра сертификации  
открытых ключей высшего уровня

**Структура заявки на сертификацию открытого ключа уполномоченного лица  
центра сертификации второго уровня в форме электронного документа**

Заявка на сертификацию открытого ключа уполномоченного лица центра сертификации второго уровня в форме электронного документа содержит следующие базовые поля:

<b>Наименование (на англ. языке)</b>	<b>Описание</b>
N (Name)	Фамилия, имя уполномоченного лица центра сертификации
IDNP	Идентификационный номер физического лица – уполномоченного лица центра сертификации
CN (Common Name)	Наименование центра сертификации
L (Locality)	Город
S (State)	Государство
OU (Organizational Unit)	Подразделение юридического лица
O (Organization)	Наименование юридического лица
T (Title)	Должность уполномоченного лица центра сертификации
C (Country)	Код государства
E (Email address)	Адрес электронной почты уполномоченного лица центра сертификации
OID (Certificate Template)	Шаблон сертификата
CryptoProvider	Средства цифровой подписи
Public Key	Сертифицируемый открытый ключ
FileName	Имя файла, куда помещается запрос на сертификацию
Street address	Адрес центра сертификации
Postal code	Почтовый код центра сертификации
Phone, Fax	Телефон, факс центра сертификации
Остальные процедуры генерации запроса на сертификацию проходят в соответствии с RFC 2986	

Приложение № 5  
к Регламенту Центра сертификации  
открытых ключей высшего уровня

**Структура сертификата открытого ключа  
уполномоченного лица центра сертификации второго уровня**

Сертификат открытого ключа уполномоченного лица центра сертификации второго уровня содержит следующие поля:

Наименование (на англ. языке)	Описание	Содержание
<i>Базовые поля</i>		
Version	Версия	V3
Serial Number	Отдельный регистрационный номер сертификата	Номер
Issuer	Идентификационные данные Центра сертификации высшего уровня	N = Фамилия, имя уполномоченного лица Центра сертификации высшего уровня, IDNP  CN = MoldovaCA  L = Кишинэу  S = Республика Молдова  OU = Центр сертификации высшего уровня  O = Служба информации и безопасности Республики Молдова, IDNO  P = Телефон уполномоченного лица  T = Должность уполномоченного лица Центра сертификации высшего уровня  C = MD  E = pki@sis.md
Validity Period	Срок действия сертификата	Действителен с: " __ " ____ 20__ г. чч:мм:сс GMT  Действителен по: " __ " ____ 20__ г. чч:мм:сс GMT

Subject	Идентификационные данные центра сертификации второго уровня	<p>N = Фамилия, имя уполномоченного лица центра сертификации второго уровня, IDNP</p> <p>CN = Наименование центра сертификации второго уровня</p> <p>L = Кишинэу</p> <p>S = Республика Молдова</p> <p>OU = Подразделение юридического лица, управляющее центром сертификации второго уровня</p> <p>O = Наименование юридического лица, управляющего центром сертификации второго уровня</p> <p>P = Телефон уполномоченного лица</p> <p>T = Должность уполномоченного лица центра сертификации второго уровня</p> <p>C = MD</p> <p>E = ___@____.____</p>
FriendlyName	Понятное имя	Понятное имя центра сертификации второго уровня (по выбору центра сертификации второго уровня)
Public Key	Открытый ключ уполномоченного лица центра сертификации второго уровня	Открытый ключ (алгоритм ____)
Subject Signature Algorithm	Алгоритм подписи владельца сертификата	Хэш-функция/алгоритм подписи
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	SHA-1/RSA
Issuer Sign	Цифровая подпись издателя сертификата	Подпись издателя в соответствии с SHA-1/RSA

<i>Дополнительные поля</i>		
Key Usage	Использование ключа	Неотрекаемость, Цифровая подпись в сертификате уполномоченного лица центра сертификации второго уровня, Цифровая подпись в списке отозванных сертификатов (CRL)
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа уполномоченного лица Центра сертификации высшего уровня, соответствующего данному сертификату
PrivateKeyUsagePeriod	Период действия закрытого ключа	Действителен с: " __ " ____ 20__ г. чч:мм:сс GMT Действителен по: " __ " ____ 20__ г. чч:мм:сс GMT
CRL Distribution Point	Точка распределения списка отозванных сертификатов (CRL)	URL= <a href="http://www.pki.sis.md/cert/rootca.crl">http://www.pki.sis.md/cert/rootca.crl</a>
Certificate Template	Шаблон сертификата	SubCA

Приложение № 6  
к Регламенту Центра сертификации  
открытых ключей высшего уровня

**Образец заявления на приостановление действия сертификата открытого ключа  
уполномоченного лица центра сертификации второго уровня**

**Центру сертификации открытых  
ключей высшего уровня**

**Заявление  
на приостановление действия сертификата открытого ключа**

Настоящим, \_\_\_\_\_,  
(фамилия, имя уполномоченного лица)  
Номер документа, удостоверяющего личность: \_\_\_\_\_,  
IDNP: \_\_\_\_\_,  
Регистрационный номер в центре сертификации \_\_\_\_\_,  
являясь уполномоченным лицом \_\_\_\_\_,  
\_\_\_\_\_ (наименование центра сертификации второго уровня)  
свидетельство о регистрации № \_\_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 200\_\_ г.,  
прошу приостановить действие сертификата открытого ключа, выданного на мое имя,  
№ \_\_\_\_\_  
на срок \_\_\_\_\_ дней,  
(количество дней прописью)  
в связи с \_\_\_\_\_.  
(причина приостановления)

Уполномоченное лицо центра сертификации  
\_\_\_\_\_  
(подпись) / \_\_\_\_\_  
(фамилия, имя)

Руководитель центра сертификации  
\_\_\_\_\_  
(подпись) / \_\_\_\_\_  
(фамилия, имя)

м.п.

" \_\_\_\_ " \_\_\_\_\_ 200\_\_ г.

Приложение № 7  
к Регламенту Центра сертификации  
открытых ключей высшего уровня

**Образец заявления на возобновление действия сертификата открытого ключа  
уполномоченного лица центра сертификации второго уровня**

**Центру сертификации открытых  
ключей высшего уровня**

**Заявление  
на возобновление действия сертификата открытого ключа**

Настоящим, \_\_\_\_\_,  
(фамилия, имя уполномоченного лица)

Номер документа, удостоверяющего личность: \_\_\_\_\_,

IDNP: \_\_\_\_\_,

Регистрационный номер в центре сертификации \_\_\_\_\_,

являясь уполномоченным лицом \_\_\_\_\_,

\_\_\_\_\_

(наименование центра сертификации второго уровня)

свидетельство о регистрации № \_\_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 200\_\_ г.,

прошу возобновить действие сертификата открытого ключа, выданного на мое имя,

№ \_\_\_\_\_,

приостановленного на \_\_\_\_\_ дней,

(количество дней прописью)

в связи с \_\_\_\_\_.

(причина приостановления)

Обоснование для возобновления действия сертификата открытого ключа \_\_\_\_\_

\_\_\_\_\_.

" \_\_\_\_ " \_\_\_\_\_ 200\_\_ г.

Уполномоченное лицо центра сертификации

\_\_\_\_\_/\_\_\_\_\_  
(подпись) (фамилия, имя)

Руководитель центра сертификации

\_\_\_\_\_/\_\_\_\_\_  
(подпись) (фамилия, имя)

м.п.

**Образец заявления на отзыв сертификата открытого ключа уполномоченного  
лица центра сертификации второго уровня**

**Центру сертификации открытых  
ключей высшего уровня**

**Заявление  
на отзыв сертификата открытого ключа**

Настоящим, \_\_\_\_\_,  
(фамилия, имя уполномоченного лица)

Номер документа, удостоверяющего личность: \_\_\_\_\_,

IDNP: \_\_\_\_\_,

Регистрационный номер в центре сертификации \_\_\_\_\_,  
являясь уполномоченным лицом \_\_\_\_\_

\_\_\_\_\_,  
(наименование центра сертификации второго уровня)

свидетельство о регистрации № \_\_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 200\_\_ г.,

прошу отозвать сертификат открытого ключа, выданный на мое имя,  
№ \_\_\_\_\_

в связи с \_\_\_\_\_  
(причина отзыва)

" \_\_\_\_ " \_\_\_\_\_ 200\_\_ г.

Уполномоченное лицо центра сертификации  
\_\_\_\_\_  
(подпись) / \_\_\_\_\_  
(фамилия, имя)

Руководитель центра сертификации  
\_\_\_\_\_  
(подпись) / \_\_\_\_\_  
(фамилия, имя)

м.п.

Приложение № 9  
к Регламенту Центра сертификации  
открытых ключей высшего уровня

**Образец заявления на подтверждение подлинности  
и действительности сертификата открытого ключа**

**Центру сертификации открытых  
ключей высшего уровня**

**Заявление**

**на подтверждение подлинности и действительности сертификата открытого ключа**

Настоящим, \_\_\_\_\_,  
(фамилия и имя заявителя)

Номер документа, удостоверяющего личность \_\_\_\_\_,

Контактные данные \_\_\_\_\_  
\_\_\_\_\_.

прошу подтвердить подлинность и действительность сертификата открытого ключа  
регистрационный номер № \_\_\_\_\_,  
выданного на имя \_\_\_\_\_.  
(фамилия и имя)

К настоящему заявлению прилагается сертификат открытого ключа  
регистрационный номер № \_\_\_\_\_,  
выданный на имя \_\_\_\_\_.  
(фамилия и имя)

в форме электронного документа на материальном носителе \_\_\_\_\_.  
(тип и номер носителя)

"\_\_" \_\_\_\_\_ 200\_\_ г.

\_\_\_\_\_/\_\_\_\_\_  
(подпись) (фамилия, имя)

**Технологические характеристики  
программно-технического комплекса Центра сертификации высшего уровня**

№ п/п	Критерий	Технологические характеристики
1.	Способы сертификации	Сетевая, иерархическая
2.	Множественные службы сертификации	Без ограничений
3.	Множественные службы регистрации	Без ограничений
4.	Масштабируемость	Количество выпущенных сертификатов без ограничений
5.	Формат сертификата и списка отозванных сертификатов	В соответствии с ISO/IEC 9594/8 Directory Services (X.509 v3) RFC 3280 (бывший RFC 2459) Certificate and Certificate Revocation List (CRL) Profile
6.	Дополнения сертификата	X.509 v 3, PKIX, FPKX, Web, SET, VPN, определяемые пользователем
7.	Формат сертификата ограниченного использования	В соответствии с RFC 3039
8.	Формат атрибутного сертификата для авторизации	В соответствии с RFC 3281
9.	Политика применения сертификата и структура регламента	В соответствии с RFC 2527 Certificate Policy and Certification Practices Framework
10.	Протоколы управления сертификатами	В соответствии с RFC 2510 Certificate Management Protocols (CMP)
11.	Запрос на сертификацию	В соответствии с RFC 2986 Certification Request Syntax Specification
12.	Протокол определения статуса сертификата	В соответствии с RFC 2560 Online Certificate Status Protocol (OCSP)

13.	Методы отзыва сертификата	Посредством распространения списков отозванных сертификатов, протокол OCSP
14.	Получение из реестра сертификатов и списка отозванных сертификатов	В соответствии с RFC 2585 HTTP/FTP Operations Автоматическая рассылка списков отозванных сертификатов по электронной почте
15.	Управление сертификатами на базе сообщений управления сертификатами	В соответствии с RFC 2797 Certificate Management Messages over CMS (CMC)
16.	Алгоритмы и идентификаторы для профилей сертификатов и списка отозванных сертификатов САС PKIX	В соответствии с RFC 3279 (бывший RFC 2528) Algorithms and Identifiers for Internet X.509 Public Key Infrastructure Certificate and CRL Profile
17.	Поддерживаемые алгоритмы цифровой подписи	RFC3447 – Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1; ГОСТ Р 34.10-94 ГОСТ Р 34.10-2001
18.	Поддерживаемые алгоритмы функции хеширования	RFC3174 – US Secure Hash Algorithm 1 (SHA1) ГОСТ Р 34.11-94
19.	Протоколы сервера сертификации и проверки достоверности данных	В соответствии с RFC 3029 Data Validation and Certification Server Protocols
20.	Эксплуатационные протоколы инфраструктуры открытых ключей	В соответствии с RFC 2559 LDAP v2
21.	Схема поддержки PKIX в среде LDAP v2	В соответствии с RFC 2587 LDAP v2 Schema
22.	Коммуникации с клиентом (подсистемы получения сертификатов)	PKCS#10/7, PKCS#12, посредством считывания PIN-кода, по электронной почте, SSL, PKIX-CMP
23.	Коммуникации между подсистемами сертификации и регистрации	Подписанные сообщения, PKIX-CMP
24.	Механизмы регистрации	Личное присутствие пользователя, посредством Web, электронная почта, VPN соединение

25.	Поддержка каталогов	Собственный каталог или поддержка любого каталога LDAP v2 и v3
26.	Поддержка смарт-карт	Стандарты: ISO 7816-1/2/3, PKCS#11, PC/SC, другие распространенные стандарты смарт-карт
27.	Восстановление ключей	Возможность резервирования администраторских и пользовательских ключей
28.	Протоколы проставления меток времени	В соответствии с RFC 3161 Time-Stamp Protocol (TSP)
29.	Управление безопасностью жизненного цикла сертификации	Отказоустойчивость при проверке статуса сертификата Гарантированность обслуживания пользователей Создание системы контроля над всеми действиями администратора с сертификатом, контроль целостности сертификата
30.	Обеспечение целостности баз данных сертификатов, владельцев сертификатов и др.	Использование концепции надежной компьютерной базы, дискреционное и мандатное управление доступом, метки, повторное использование объекта, достоверный маршрут; создание системы резервного копирования
31.	Обеспечение безопасности закрытых ключей	Безопасное создание, хранение, использование, многофакторная система аутентификации
32.	Контроль безопасности	Регистрация и контроль событий в подсистемах Ведение, обработка и проверка контрольных журналов Обеспечение защиты контрольных журналов от несанкционированных изменений и уничтожения