Одобрено
Решением Правления
№ 3-0721-04 от 21.07.2022 г.

Утверждено
Постановлением Совета Директоров
№ 3-0729-01 от 29.07.2022 г.

ПОЛИТИКА
применения регистрационных свидетельств удостоверяющего центра АО «Банк ЦентрКредит»

Содержание

Глава 1. Введение

Раздел 1.1. Общие положения

1. Настоящая Политика применения регистрационных свидетельств удостоверяющего центра АО «Банк ЦентрКредит» (далее – Политика регистрационных свидетельств) разработана в соответствии с требованиями правовых актов Республики Казахстан по вопросам электронного документа и электронной цифровой подписи в целях обеспечения функционирования Удостоверяющего центра АО «Банк ЦентрКредит» (далее – Удостоверяющий центр).

2. Настоящая Политика регистрационных свидетельств разработана с учетом международных отраслевых рекомендаций RFC 3647 «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework» (Структура документов политики и практики сертификатов в интернет инфраструктуре открытых ключей формата X.509).

3. Настоящая Политика регистрационных свидетельств определяет виды регистрационных свидетельств, выпускаемых Удостоверяющим центром, основные принципы и общие требования их применимости в заинтересованных информационных системах, объединенных типовыми требованиями информационной безопасности, что гарантирует определенный уровень доверия в информационных системах, использующих эти регистрационные свидетельства.

4. Настоящая Политика регистрационных свидетельств не определяет детальный порядок и процедуры функционирования Удостоверяющего центра, обеспечения безопасности инфраструктуры открытых ключей, которые согласно требованиям правовых актов Республики Казахстан и международных отраслевых рекомендаций RFC 3647 вынесены в отдельные внутренний нормативный документ (далее – Регламент деятельности удостоверяющего центра АО «Банк ЦентрКредит»).

5. С момента подписания участником информационной системы, использующей сервисы Удостоверяющего центра, заявления на выпуск регистрационного свидетельства, для участника становятся обязательными к выполнению применимые к нему требования Политики регистрационных свидетельств и Регламента деятельности удостоверяющего центра АО «Банк ЦентрКредит», ссылка на которые содержится в подписанном заявлении.

6. Исчерпывающий перечень видов регистрационных свидетельств, выпускаемых Удостоверяющим центром для подписчиков, с указанием идентифицирующих их признаков (профилей) определяется Разделом 1.1 Регламента деятельности удостоверяющего центра АО «Банк ЦентрКредит».

Раздел 1.2. Наименование и атрибуты документа

7. Документ именуется «Политика применения регистрационных свидетельств удостоверяющего центра АО «Банк ЦентрКредит»», как этого требует правовой акт по вопросам аккредитации удостоверяющих центров, изданный уполномоченным органом в сфере обеспечения информационной безопасности[1].

8. Редакция документа 1.0.0.

9. Политика регистрационных свидетельств в настоящей редакции введена в действие протокольным решением Совета директоров Банка от 29.07.2022 года № 3-0729-01.

10. Действующая редакция Политики регистрационных свидетельств публикуется на официальном информационном ресурсе Банка в сети Интернет.

11. Политика регистрационных свидетельств зарегистрирована в дереве международных объектных идентификаторов с присвоением объектного идентификатора.

Раздел 1.3. Участники инфраструктуры открытых ключей Банка

12. Удостоверяющий центр – структурное подразделение Банка, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной

[1] На дату утверждения Политики регистрационных свидетельств действует приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан «Об утверждении Правил проведения аккредитации удостоверяющих центров» от 1 июня 2020 года №224/НҚ.

цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства[2].

13. Центры регистрации Удостоверяющего центра – отделения и/или уполномоченные выделенные работники Банка, ответственные за прием документов на выпуск или отзыв регистрационных свидетельств, идентификацию заявителей и предоставление заявителям доступа к готовым регистрационным свидетельствам.

14. Владелец регистрационного свидетельства (или подписчик Удостоверяющего центра) – физическое или юридическое лицо, действующее в лице своего уполномоченного представителя, как субъект, на имя которого Удостоверяющим центром выдано регистрационное свидетельство, правомерно владеющий закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве.

15. Доверяющие стороны (или пользователи регистрационных свидетельств) – владельцы регистрационных свидетельств, или любые другие субъекты, которые действуют, полагаясь на регистрационные свидетельства, выпущенные Удостоверяющим центром, и/или электронные документы с электронными цифровыми подписями, подлинность которых проверяется с помощью этих регистрационных свидетельств.

Раздел 1.4. Назначение регистрационных свидетельств

16. Удостоверяющий центр выпускает регистрационные свидетельства различного назначения.

17. Основной целью выпуска регистрационных свидетельств Удостоверяющим центром является обеспечение потребностей информационных систем, принадлежащих Банку. Вместе с тем, регистрационные свидетельства, выпущенные Удостоверяющим центром, могут применяться заинтересованными информационными системами иных владельцев.

18. При этом Удостоверяющий центр Банка запрещает использование выпущенных им регистрационных свидетельств в информационных системах, связанных с управлением источниками повышенной опасности (ядерным, аэронавигационным оборудованием, системами контроля вооружений и др.), а также в иных информационных системах в любых случаях, когда ошибка при принятии решения о доверии, основанном на регистрационном свидетельстве, может повлечь за собой ранение или смерть персонала, или ущерб окружающей среде.

19. Назначение регистрационного свидетельства определяется целью использования пары криптографических ключей, открытый ключ которой удостоверен регистрационным свидетельством.

20. Закрепленная цель использования пары криптографических ключей фиксируется в каждом регистрационном свидетельстве, выпускаемом Удостоверяющим центром для участника, в расширении «keyUsage» и/или «extendedKeyUsage».

21. Кроме этого, область допустимого применения выпускаемых Удостоверяющим центром регистрационных свидетельств может дополнительно подразделяться с помощью объектных идентификаторов политики, которые фиксируются в расширении регистрационного свидетельства «cerificatePolicies».

22. Наличие объектных идентификаторов политики дает информационным системам, использующим регистрационные свидетельства, возможность дополнительной защиты в форме контроля системой наборов необходимых и запрещенных политик с ограничением применения неподходящих регистрационных свидетельств.

23. Не допускается использование регистрационных свидетельств, выпущенных Удостоверяющим центром, способами, противоречащими законодательству Республики Казахстан, Политике регистрационных свидетельств, Регламенту деятельности удостоверяющего центра АО «Банк ЦентрКредит».

24. Регистрационные свидетельства подписчиков Удостоверяющего центра используются для работы с программным обеспечением доверяющих сторон и не используются как технологические регистрационные свидетельства информационной системы Удостоверяющего центра. В свою очередь технологические регистрационные

[2] На дату утверждения Политики регистрационных свидетельств данный функционал выполняет Дирекция криптографической защиты информации Центра обеспечения информационной безопасности Банка.

свидетельства информационной системы Удостоверяющего центра не используются ни для каких иных целей кроме их прямого функционального назначения.

Раздел 1.5. Управление документом

25. Политика регистрационных свидетельств актуализируется Удостоверяющим центром, расположенным по адресу: A05G1D2, г. Алматы, ул. Панфилова, д. 98, блок Б.

26. Контактное лицо по вопросам актуализации документа – Руководитель Удостоверяющего центра, A05G1D2, г. Алматы, ул. Панфилова, д. 98, блок Б, +7 (727) 2-598-583 (вн. 12921), alexey.korobetskikh@bcc.kz.

27. Изменения и дополнения в Политику регистрационных свидетельств готовятся Удостоверяющим центром либо в форме новой редакции, либо в форме перечня изменений и дополнений к текущей редакции Политики регистрационных свидетельств.

28. Перед утверждением изменения и дополнения в Политику регистрационных свидетельств проходят согласование с заинтересованными подразделениями и должностными лицами Банка согласно внутренним процедурам.

29. Изменения и дополнения в Политику регистрационных свидетельств утверждаются протокольным решением Совета директоров Банка.

30. Все изменения и дополнения в Политику регистрационных свидетельств публикуются на официальном информационном ресурсе Банка в сети Интернет.

31. Публикация новой утвержденной редакции Политики регистрационных свидетельств является официальным уведомлением о вступлении ее в силу для пользователей всех регистрационных свидетельств, выпущенных Удостоверяющим центром, включая их владельцев.

32. С даты публикации новой редакции Политики регистрационных свидетельств, если иное не предусмотрено переходными положениями утверждающего решения, изменения и дополнения становится обязательными для применения пользователями всех регистрационных свидетельств, выпущенных Удостоверяющим центром, включая их владельцев.

Раздел 1.6. Термины, определения и сокращения

33. В Политике регистрационных свидетельств используются следующие понятия:

1) аутентификация – процесс или сервис безопасности, реализующий этот процесс, который предназначен для проверки того, что лицо (предмет) является тем, кем себя именует (чем он поименован);

2) Банк – АО «Банк ЦентрКредит»;

3) данные активации – любые данные, за исключением криптографических ключей, которые необходимы для выполнения криптографических операций и требуют защиты: персональные идентификационные номера (PIN), парольные фразы, компоненты разделенного криптографического ключа, биометрические параметры и др.;

4) дерево международных объектных идентификаторов – стандартизированный ITU-T и ISO/IEC механизм (X.660) именования любых реальных или абстрактных объектов однотипными недвусмысленными всеобъемлющими именами, предназначенный для регистрации имен с помощью трех иерархических деревьев особой формы (от 3 разных корней), в которых каждый последующий узел наделен целочисленным номером и ответственен за дальнейшее выделение и регистрацию ветвей, исходящих от него самого;

5) закрытый ключ электронной цифровой подписи – последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи;

6) закрытый криптографический ключ – в криптосистемах с открытым ключом, тот ключ из ключевой пары, который известен только подписчику[3];

7) идентификация – в контексте Политики регистрационных свидетельств, процесс (или результат процесса), который устанавливает идентичность физического или юридического лица (показывающий, что данное лицо является однозначно определенным

[3] Закрытые ключи электронной цифровой подписи являются одной из разновидностей закрытых криптографических ключей.

реально существующим лицом), и состоит из двух этапов:

установление соответствия предъявленного лицом имени реально существующей идентичности лица и

установление того, что лицо, обращающееся за доступом к чему-либо от определенного имени, на самом деле является тем лицом, которым себя именует (аутентификация);

8) инфраструктура открытых ключей – набор сил и средств (технических, материальных, людских и пр.), распределённых служб и компонентов, в совокупности используемых для решения криптографических задач (аутентификации, шифрования, контроля целостности и доказательности) на основе криптосистем с открытым ключом, способный самостоятельно обеспечить управление открытыми ключами, посредством которых решаются указанные задачи;

9) компрометация криптографических ключей – утрата владельцем криптографических ключей уверенности в том, что конкретные криптографические ключи обеспечивают безопасность защищаемой с их помощью информации;

10) носитель ключевой информации – в контексте настоящего Регламента, съемный машинный носитель информации (специализированный аппаратный токен, карта памяти, жесткий диск и др.), способный хранить криптографические ключи в электронной форме;

11) объектный идентификатор – идентификатор, который однозначно именует узел дерева международных объектных идентификаторов в форме списка целочисленных значений, упорядоченного от корня дерева к данному узлу;

12) открытый ключ электронной цифровой подписи – последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе;

13) открытый криптографический ключ – в криптосистемах с открытым ключом, тот ключ из ключевой пары, который известен публике[4];

14) политика применения регистрационных свидетельств (также именуется Политикой регистрационных свидетельств) – нормативный документ, который представляет собой озаглавленный набор правил, определяющих применимость регистрационного свидетельства в определенной общности (классе) приложений с общими требованиями информационной безопасности;

15) регламент деятельности удостоверяющего центра – нормативный документ, который определяет порядок организации основной деятельности удостоверяющего центра, осуществляемой в соответствии с Политикой регистрационных свидетельств, включая течение основных процессов Удостоверяющего центра;

16) регистрационное свидетельство – электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом Республики Казахстан “Об электронном документе и электронной цифровой подписи”;

17) сертификат открытого (криптографического) ключа (далее - сертификат) – открытый криптографический ключ подписчика вместе с дополнительной информацией, идентифицирующей этот ключ и подписчика, подлинность и взаимосвязь которых удостоверена электронной цифровой подписью, сформированной закрытым криптографическим ключом Удостоверяющего центра[5];

---

[4] Открытые ключи электронной цифровой подписи являются одной из разновидностей открытых криптографических ключей.

[5] Понятие “сертификат” введено в соответствии с международным стандартом ITU-T X.509 “Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks” (Информационная технология – Взаимодействие открытых систем – Справочник: структуры сертификатов открытых (криптографических) ключей и атрибутов). Регистрационные свидетельства, выпускаемые Удостоверяющим центром в соответствии с Законом Республики Казахстан “Об электронном документе и электронной цифровой подписи”, являются одной из разновидностей выпускаемых сертификатов. Вместе с тем, в законодательных актах Республики Казахстан не используется терминов, равносильных термину “сертификат открытого (криптографического) ключа”.

В связи с этим, всюду в тексте Политики регистрационных свидетельств термин “регистрационные свидетельства”, введенный в Законе Республики Казахстан “Об электронном документе и электронной цифровой подписи”, обобщает все возможные разновидности сертификатов открытых (криптографических) ключей,

18) список отозванных регистрационных свидетельств (CORC) – часть регистра регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва;

19) средства криптографической защиты информации (или СКЗИ) – средства, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами;

20) средства электронной цифровой подписи – совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи[6];

21) токен – в контексте Политики регистрационных свидетельств, физическое устройство, выдаваемое уполномоченному лицу в целях организации защищенного хранения резервной копии закрытых криптографических ключей и настроек аппаратных криптографических модулей (Hardware Security Module, HSM) Удостоверяющего центра;

22) участники инфраструктуры открытых ключей – совокупность физических и юридических лиц, действующих в лице своих уполномоченных представителей, которые выполняют любую из ролей: пользователя или владельца регистрационного свидетельства (доверяющей стороны или подписчика), центра регистрации или удостоверяющего центра, – в одной и той же инфраструктуре открытых ключей;

23) центр регистрации Удостоверяющего центра – подразделения и/или уполномоченные выделенные работники Банка, ответственные за прием документов на выпуск или отзыв регистрационных свидетельств, идентификацию заявителей и предоставление заявителям доступа к готовым регистрационным свидетельствам;

24) цепочка регистрационных свидетельств – упорядоченная последовательность регистрационных свидетельств, начинающаяся с регистрационного свидетельства, электронная цифровая подпись в котором может быть проверена с помощью доверенного корневого регистрационного свидетельства, успешная обработка которой с помощью стандартизированного алгоритма позволяет подтвердить принадлежность открытого криптографического ключа лицу, указанному в заключительном регистрационном свидетельстве последовательности, в поле “subject”;

25) электронная цифровая подпись (или ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

26) электронный документ – документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством ЭЦП.

Глава 2. Ответственность за хранилище и публикацию данных в нем

Раздел 2.1. Хранилище

34. Деятельность Удостоверяющего центра требует непрерывного размещения в оперативном доступе актуальных данных реестра регистрационных свидетельств, выпущенных Удостоверяющим центром, и информации об их статусе.

35. В связи с этим, составной частью информационной системы Удостоверяющего центра является хранилище, которое Удостоверяющий центр использует в качестве справочника информации при предоставлении своих основных сервисов.

36. Кроме этого, Удостоверяющий центр ведет раздел на официальном информационном ресурсе Банка в сети Интернет, в котором также публикует регистрационные свидетельства Удостоверяющего центра и ссылки для доступа к спискам отозванных регистрационных свидетельств, а также необходимый минимум нормативных документов и других данных о своих сервисах (включая Политику регистрационных свидетельств и Регламент деятельности удостоверяющего центра).

выпускаемых Удостоверяющим центром Банка, т.е. его следует раскрывать как “регистрационные свидетельства и (или) сертификаты открытых (криптографических) ключей иного назначения”.

[6] Средства электронной цифровой подписи являются одной из разновидностей средств криптографической защиты информации.

Раздел 2.2. Публикация в хранилище информации о регистрационных свидетельствах

37. Основным протоколом информационного взаимодействия с хранилищем Удостоверяющего центра является облегченный протокол доступа к службам каталогов в версии, определенной рекомендациями RFC 2251 (Lightweight Directory Access Protocol v.3, версия 3).

38. Данный протокол позволяет обращаться в режиме онлайн в хранилище Удостоверяющего центра с запросами о наличии регистрационных свидетельств, и получать их содержимое.

39. Любые исключения из этих требований, в случае их возникновения, должны быть включены в Регламент деятельности удостоверяющего центра и опубликованы в свободном доступе владельцев и пользователей регистрационных свидетельств (подписчиков и доверяющих сторон).

Раздел 2.3. Периодичность актуализации данных в хранилище

40. Удостоверяющий центр публикует каждое вновь выпущенное регистрационное свидетельство в хранилище.

41. В случае отзыва регистрационного свидетельства Удостоверяющий центр удаляет его в порядке, определенном в разделе 2.3 Регламента деятельности удостоверяющего центра АО «Банк ЦентрКредит».

42. В случае отзыва любого регистрационного свидетельства Удостоверяющий центр формирует и публикует в хранилище обновленный список отозванных регистрационных свидетельств.

43. Отозванные регистрационные свидетельства удаляются из списков отозванных регистрационных свидетельств по факту истечения срока действия регистрационного свидетельства.

44. В условиях отсутствия событий отзыва новые списки отозванных регистрационных свидетельств формируются и выпускаются на регулярной основе.

Раздел 2.4. Контроль доступа к хранилищу

45. Доступ для чтения данных из хранилища Удостоверяющий центр разрешается любому пользователю, опосредованно, через обслуживаемые информационные системы Банка, без ограничений постоянного характера.

46. Доступ для добавления данных в хранилище, изменения данных в хранилище или исключения (удаления) данных из хранилища запрещен Удостоверяющим центром для неуполномоченных на то лиц.

47. В случаях кибератак, иных угроз перебоя в предоставлении сервисов или обоснованных подозрений в них Удостоверяющий центр оставляет за собой право применять временные ограничения доступа для чтения данных из хранилища в качестве активных мер противодействия.

48. Ограничения и контроли доступа в хранилище применяются в соответствии с Политикой информационной безопасности Банка[7] (далее – Политика информационной безопасности).

Глава 3. Идентификация и аутентификация

Раздел 3.1. Требования к именам

49. Удостоверяющий центр использует правила именования субъектов, призванные обеспечить однозначную идентификацию подписчиков во всех выпускаемых регистрационных свидетельствах.

50. Однозначность идентификации достигается за счет максимально возможного использования идентификационных номеров из единого республиканского реестра (ИИН и БИН).

---

[7] Политика информационной безопасности опубликована на официальном ресурсе Банка в сети Интернет по адресу https://www.bcc.kz/product/information-security/

51. В случае отсутствия у физического лица ИИН, вместо него используются номер и другие реквизиты паспорта, при отсутствии паспорта – документа, заменяющего паспорт.

52. В случае отсутствия у юридического лица БИН, вместо него используется номер и реквизиты документа о регистрации плательщика НДС (VAT).

53. В рамках, установленных Регламентом деятельности удостоверяющего центра, в состав имен помимо идентификационных номеров допускается включение фамилии, имени, отчества, торговой марки, названия информационной системы, аббревиатуры организационно-правовой формы, названия организации и других общепринятых и понятных для человеческого восприятия имен и названий.

54. Анонимность владельцев регистрационных свидетельств не допускается.

55. Использование владельцами регистрационных свидетельств псевдонимов вместо общеизвестных имен не допускается.

56. Заявители на выпуск регистрационных свидетельств не должны использовать в своих заявлениях имена, нарушающие права их законных правообладателей. Удостоверяющий центр не несет ответственности за проверку на предмет правообладания заявителя именем, указанным в заявлении, и не вступает в споры и разбирательства, связанные с собственностью на доменные, торговые и тому подобные имена и марки.

57. Удостоверяющий центр оставляет за собой право отклонить любое заявление на выпуск регистрационного свидетельства или приостановить его рассмотрение, если ему становится известно о факте подобного спора или разбирательства.

58. Содержание поля «Issuer» всех регистрационных свидетельств, выпускаемых Удостоверяющим центром, определяется в соответствии с разделом 3.1 Регламента деятельности удостоверяющего центра.

59. В корневых регистрационных свидетельствах Удостоверяющего центра в поле «Subject» содержатся в точности те же данные, что и в поле «Issuer».

60. Структура содержания поля «Subject» во всех регистрационных свидетельствах, выпускаемых Удостоверяющим центром, определяется в соответствии с разделом 3.1 Регламента деятельности удостоверяющего центра.

61. Вследствие правового требования однозначной идентификации, имена всех владельцев регистрационных свидетельств являются уникальными. Вместе с тем, выпуск и использование двух и более регистрационных свидетельств с одним и тем же именем в поле «Subject» разрешается при условии, что соответствующими закрытыми криптографическими ключами владеет и пользуется одно и то же физическое лицо или представитель юридического лица.

Раздел 3.2. Первоначальная проверка идентичности

62. Первоначальная проверка идентичности – это наиболее полная форма процедур идентификации и аутентификации, которая согласно международным отраслевым рекомендациям проводится в отношении подписчика при выпуске первого регистрационного свидетельства.

63. Вместе с тем, любая последующая процедура, требующая идентификации владельца регистрационного свидетельства (отзыв действующего или выпуск нового регистрационного свидетельства), проводится по полной форме первоначальной проверки идентичности в соответствии с требованиями раздела 3.2 Регламента деятельности удостоверяющего центра.

Глава 4. Операционные требования к жизненному циклу регистрационных свидетельств

Раздел 4.1. Заявления на выпуск регистрационных свидетельств

64. Заявления на выпуск регистрационного свидетельства подают:

1) уполномоченные представители юридических лиц;
2) физические лица, действующие самостоятельно.

65. Заявления на выпуск регистрационного свидетельства подаются в центр регистрации.

66. Заявление на выпуск регистрационного свидетельства содержит ссылку на

Политику регистрационных свидетельств и Регламент деятельности удостоверяющего центра.

67. Заявление на выпуск регистрационного свидетельства является документом, означающим принятие заявителем обязательств владельца и пользователя регистрационных свидетельств (подписчика и доверяющей стороны) соблюдать принципы и выполнять требования Политики регистрационных свидетельств и Регламента деятельности удостоверяющего центра.

68. Необходимые Удостоверяющему центру обязательства владельца и пользователя регистрационных свидетельств (подписчика и доверяющей стороны) изложены в разделе 9.6 настоящей Политики регистрационных свидетельств.

Раздел 4.2. Обработка заявлений на выпуск регистрационных свидетельств

69. Срок рассмотрения и обработки заявлений на выпуск регистрационных свидетельств определяется разделом 4.2 Регламента деятельности удостоверяющего центра.

70. Зарегистрированное заявление отклоняется в случаях, установленных законодательными актами Республики Казахстан по вопросам электронного документа и электронной цифровой подписи[8] и перечисленных в разделе 4.2 Регламента деятельности удостоверяющего центра.

71. Перед регистрацией заявления на выпуск регистрационного свидетельства проводится идентификация и аутентификация заявителя.

72. Заявление на выпуск регистрационного свидетельства не регистрируется, если:

1) заявитель при подаче заявления в установленный срок не прошел успешно процедуру идентификации и аутентификации, в т.ч. не предоставил документальных доказательств достоверности информации, указанной в заявлении;

2) заявитель не обладает или не имеет возможности использовать средство электронной цифровой подписи, совместимое с сервисами Удостоверяющего центра.

73. Все зарегистрированные заявления на выпуск регистрационных свидетельств, не отклоненные по вышеуказанным основаниям, подлежат удовлетворению в установленный срок.

Раздел 4.3. Выпуск регистрационных свидетельств

74. Каждое регистрационное свидетельство создается Удостоверяющим центром по факту регистрации и успешной обработки отдельного заявления на выпуск регистрационного свидетельства в центре регистрации.

75. Выпуску любого регистрационного свидетельства подписчику Удостоверяющего центра предшествуют следующие этапы:

1) идентификация личности подписчика, а также, если требуется, проверка его полномочий представлять юридическое лицо;

2) защищенная генерация ключевой пары подписчика в центре регистрации;

3) защищенная доставка открытого криптографического ключа подписчика из центра регистрации в Удостоверяющий центр;

4) проверка Удостоверяющим центром факта владения подписчиком закрытым криптографическим ключом, соответствующим открытому криптографическому ключу, который подлежит регистрации Удостоверяющим центром.

76. При выпуске регистрационного свидетельства Удостоверяющий центр основывается на информации из заявления, которую успешно проверил центр регистрации в ходе процедур идентификации и аутентификации.

77. Любое регистрационное свидетельство, выпущенное Удостоверяющим центром, автоматически публикуется в хранилище.

Раздел 4.4. Принятие регистрационных свидетельств

78. После выпуска регистрационного свидетельства всем подписчикам предоставляется право в течение 14 календарных дней с даты выпуска заявить Удостоверяющему центру об отказе от намерения иметь это регистрационное свидетельство или о несогласии с его

[8] Закон Республики Казахстан “Об электронном документе и электронной цифровой подписи”, статья 14-1.

содержанием, при условии, что соответствующий закрытый криптографический ключ с момента выпуска регистрационного свидетельства до заявления об отказе не использовался подписчиком.

79. Для реализации указанного права заявителю необходимо обратиться в центр регистрации с письменным заявлением (на бумажном носителе) об отзыве регистрационного свидетельства.

80. Если подписчик не использует указанное право, то регистрационное свидетельство автоматически считается принятым подписчиком.

81. Если подписчик, не заявляя о своем отказе от намерения иметь регистрационное свидетельство или о несогласии с его содержанием, до истечения предоставляемого Удостоверяющим центром 14-дневного срока начинает использовать соответствующий закрытый криптографический ключ, то регистрационное свидетельство автоматически считается принятым подписчиком с момента первого использования закрытого ключа.

Раздел 4.5. Использование регистрационных свидетельств и ключевых пар

82. Прежде чем, предпринять любой акт, основываясь на доверии к регистрационному свидетельству, выпущенному Удостоверяющим центром, доверяющая сторона самостоятельно проверяет каждый соответствующий электронный документ, в частности, каждую имеющуюся в нем ЭЦП, а также связанные с ней регистрационные свидетельства, метки времени, квитанции (ответы службы) OCSP[9] или списки отозванных регистрационных свидетельств.

83. Для проведения проверки ЭЦП доверяющая сторона:

1) определяет и проверяет цепочку регистрационных свидетельств, которая позволяет установить субъекта, сформировавшего ЭЦП. В ходе проверки цепочки регистрационных свидетельств используется алгоритм, изложенный в рекомендациях RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” (Профиль сертификата и списка отозванных сертификатов интернет инфраструктуры открытых ключей формата X.509);

2) в ходе проверки каждого регистрационного свидетельства цепочки дополнительно контролирует содержание расширений “keyUsage” и “extendedKeyUsage” на соответствие цели использования;

3) самостоятельно проверяет наличие у подписавшего лица полномочий, достаточных для подписания электронного документа. Информационная система Удостоверяющего центра сервисов контроля полномочий подписчика не предоставляет.

84. Если любой шаг проверки дает отрицательный результат или его невозможно выполнить, то ЭЦП полагается недействительной, и электронный документ отвергается.

85. Если в электронном документе имеется отметка времени, сформированная Удостоверяющим центром, то для выполнения действия, требующего доверия к отметке времени, необходимо также проверить эту отметку времени в порядке, аналогичном проверке ЭЦП в электронном документе.

86. Если любое из регистрационных свидетельств цепочки на момент проверки ЭЦП имеет статус “отозвано”, только доверяющая сторона исключительно на свой риск решает, оправдано или нет полагаться на электронный документ, сформированный подписчиком до отзыва одного из регистрационных свидетельств цепочки. Удостоверяющий центр в случаях такого рода не несет ответственности перед пользователями регистрационных свидетельств (доверяющими сторонами), так как подача заявления на отзыв регистрационного свидетельства является обязанностью конкретного владельца регистрационного свидетельства (подписчика).

87. Если обстоятельства указывают на необходимости дополнительных гарантий со стороны авторов электронного документа, то пользователь регистрационного свидетельства (доверяющая сторона) получает такие дополнительные гарантии от владельцев

[9] OCSP – сервис для получения информации о статусе регистрационных свидетельств, выпущенных Удостоверяющим центром (согласно рекомендациям RFC 2560 “X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP”, онлайн протокол статуса сертификатов интернет инфраструктуры открытых ключей X.509).

регистрационных свидетельств (подписчиков) самостоятельно, до выполнения действий, требующих доверия к регистрационному свидетельству, и без обращения в Удостоверяющий центр.

88. Если пользователь регистрационного свидетельства (доверяющая сторона), предпринимая любой акт, основанный на доверии к регистрационному свидетельству, выпущенному Удостоверяющим центром, не выполнил вышеперечисленные условия раздела 4.5 Политики регистрационных свидетельств, то Удостоверяющий центр не несет перед доверяющей стороной ответственности за последствия такого акта.

89. Удостоверяющий центр не отвечает перед использующими регистрационные свидетельства лицами, которые не обязались выполнять требования Политики регистрационных свидетельств и Регламента деятельности удостоверяющего центра в части, касающейся обязанностей пользователя регистрационных свидетельств (доверяющей стороны), в форме письменного обязательства, электронного документа либо иной формы согласия, зафиксированной в информационной системе Банка.

90. Закрытый криптографический ключ используется владельцем регистрационного свидетельства (подписчиком) только после того, как он дал письменное обязательство выполнять обязанности подписчика и доверяющей стороны в соответствии с разделом 4.1 Политики регистрационных свидетельств, Удостоверяющий центр выпустил регистрационное свидетельство соответствующего открытого ключа, и владелец принял это регистрационное свидетельство.

91. Закрытый криптографический ключ используется подписчиком только в соответствии с законодательством, договорными обязательствами, Политикой регистрационных свидетельств и Регламентом деятельности удостоверяющего центра.

92. Использование закрытого криптографического ключа должно соответствовать содержанию расширений «keyUsage» и «extendedKeyUsage» в соответствующем регистрационном свидетельстве.

93. Владельцы регистрационных свидетельств (подписчики Удостоверяющего центра) защищают свои закрытые криптографические ключи от несанкционированного доступа и прекращают их использование после истечения срока действия или отзыва соответствующего регистрационного свидетельства.

Раздел 4.6. Обновление сроков действия в регистрационных свидетельствах

94. Услуг по обновлению сроков действия в регистрационных свидетельствах Удостоверяющий центр не предоставляет.

95. При необходимости дальнейшего использования сервисов информационной системы Банка, требующих наличия криптографических ключей, подписчик повторно проходит процедуру выпуска регистрационных свидетельств, в порядке, определенном Разделами 4.1, 4.2 и 4.3 Регламента деятельности удостоверяющего центра.

Раздел 4.7. Смена криптографических ключей в регистрационных свидетельствах

96. Услуг по смене ключей в регистрационных свидетельствах Удостоверяющий центр не предоставляет.

97. Для смены криптографических ключей подписчик повторно проходит процедуру выпуска (новых) регистрационных свидетельств, в порядке, определенном разделами 4.1, 4.2 и 4.3 Регламента деятельности удостоверяющего центра АО «Банк ЦентрКредит».

Раздел 4.8. Изменение данных в регистрационных свидетельствах

98. Услуг по изменению данных в регистрационных свидетельствах Удостоверяющий центр не предоставляет.

99. Для изменения данных в регистрационном свидетельстве подписчик повторно проходит процедуру выпуска (новых) регистрационных свидетельств, в порядке, определенном разделами 4.1, 4.2 и 4.3 Регламента деятельности удостоверяющего центра.

Раздел 4.9. Отзыв регистрационных свидетельств

100. Регистрационные свидетельства, выпущенные Удостоверяющим центром,

отзываются Удостоверяющим центром.

101. Основания для отзыва регистрационного свидетельства установлены законодательными актами Республики Казахстан по вопросам электронного документа и электронной цифровой подписи[10] и перечислены в разделе 4.9 Регламента деятельности удостоверяющего центра.

102. Отзыв регистрационного свидетельства осуществляется по заявлению, оформленному владельцем регистрационного свидетельства (подписчиком) или центром регистрации.

103. Заявления на отзыв регистрационного свидетельства подаются незамедлительно с момента обнаружения вышеуказанных оснований.

104. Перед отзывом регистрационного свидетельства центр регистрации и/или Удостоверяющий центр проверяет полномочия инициатора запрашивать отзыв, включая идентификацию заявителя. При этом применяется механизм идентификации, указанный в разделе 3.2 Политики регистрационных свидетельств.

105. Пользователи регистрационных свидетельств (доверяющие стороны) обязуются проверять статус всех регистрационных свидетельств, на которые они полагаются в своих действиях.

106. Если пользователь регистрационного свидетельства (доверяющая сторона) не использует для проверки статуса регистрационного свидетельства онлайн обращение к службе протокола OCSP, то она должна использовать для этого актуальный список отозванных регистрационных свидетельств, опубликованный в хранилище Удостоверяющего центра.

107. Списки отозванных регистрационных свидетельств являются едиными в том смысле, что они содержат отзываемые регистрационные свидетельства всех участников инфраструктуры открытых ключей: Удостоверяющего центра, центров регистрации и владельцев регистрационных свидетельств.

108. Актуальный список отозванных регистрационных свидетельств Удостоверяющего центра доступен в сети Интернет круглосуточно и непрерывно, за исключением времени плановых профилактических работ в соответствии с условиями Соглашения об уровне обслуживания Удостоверяющего центра.

109. Исключение истекших регистрационных свидетельств из списка отозванных регистрационных свидетельств осуществляется не реже интервала, определенного соответствующей настройкой информационной системы Удостоверяющего центра.

110. Новый список отозванных регистрационных свидетельств формируется и публикуется либо по факту отзыва регистрационного свидетельства любого участника инфраструктуры открытых ключей, либо по расписанию, определенному соответствующей настройкой информационной системы Удостоверяющего центра, если в течение установленного периода ни одно регистрационное свидетельство не было отозвано.

111. Вновь созданный список отозванных регистрационных свидетельств автоматически публикуется в хранилище Удостоверяющего центра незамедлительно по факту формирования.

112. Юридические лица в случае увольнения работника, имеющего доступ к закрытым криптографическим ключам, или его перевода на другой участок работы, оформляют заявление на отзыв регистрационных свидетельств, соответствующих закрытым ключам перемещаемого работника, не позднее даты перемещения. При необходимости подаются заявления на выпуск регистрационных свидетельств для другого ответственного лица.

113. Услуг по временному приостановлению или возобновлению действия регистрационных свидетельств Удостоверяющий центр не предоставляет.

114. Владелец регистрационных свидетельств (подписчик Удостоверяющего центра) имеет возможность прекратить обслуживание в Удостоверяющем центре:

1) расторгнув (все) действующий(-е) договор(-ы), предусматривающий(-е) обслуживание;

2) отзывая все действующие регистрационные свидетельства до окончания срока их действия.

115. В случае истечения срока действия всех регистрационных свидетельств подписчика

[10] Закон Республики Казахстан “Об электронном документе и электронной цифровой подписи”, статья 18, п.1.

обслуживание подписчика в Удостоверяющем центре прекращается автоматически.

116. Услуг по депонированию закрытого ключа подписчика Удостоверяющий центр не предоставляет.

117. В случае компрометации закрытых криптографических ключей Удостоверяющего центра, Удостоверяющий центр оповещает об этом владельцев всех информационных систем Банка, использующих сервисы Удостоверяющего центра.

Глава 5. Физический, операционный и управляющие контроли

Раздел 5.1. Физический контроль

118. Детальные меры физического контроля Удостоверяющего центра определены и утверждены внутренними документами Банка, и в Политике регистрационных свидетельств не раскрываются. В настоящей главе приведен общий обзор этих мер.

119. Информационная система Удостоверяющего центра обеспечена двумя центрами обработки данных (основной и резервный), расположенными на разных объектах в целях резервирования и восстановления функционирования в случае чрезвычайной ситуации.

120. Условия размещения оборудования Удостоверяющего центра в основном и резервном центрах обработки данных выбраны с учетом действующих в Республике Казахстан требований к системам бесперебойного функционирования технических средств и информационной безопасности[11].

121. Операции с криптографическими ключами Удостоверяющего центра проводятся только на физически защищенных объектах, в условиях, где затруднены и фиксируются любые попытки несанкционированного доступа, использования или раскрытия конфиденциальной информации. Остальные функции и работы Удостоверяющего центра допускается выполнять дистанционно с соблюдением требований Политики информационной безопасности и иных внутренних нормативных документов Банка по вопросам информационной безопасности.

122. Деятельность центров регистрации ведется только на физически защищенных объектах, в условиях, где затруднены и фиксируются любые попытки несанкционированного доступа, использования или раскрытия конфиденциальной информации.

123. Подразделения, реализующие меры пропускного и внутриобъектового режима в Банке, являются независимыми от Удостоверяющего центра и Центра обеспечения информационной безопасности Банка. Контроль процессов, реализующих меры пропускного и внутриобъектового режима в Банке, обеспечивается службой внутреннего аудита посредством независимой оценки в соответствии с внутренним документом Банка.

Раздел 5.2. Операционный контроль

124. Требования к уровню услуг Удостоверяющего центра со стороны заинтересованных информационных систем Банка составляют:

1) доступность сервисов – 99,5% в режиме 24/7/365, т.е. не более 1 суток 19 часов и 50 минут простоя в год, без учета плановых работ;

2) скорость обработки запросов каждого типа – не ниже 8 запросов в минуту;

3) обслуживание не менее 4 млн. регистрационных свидетельств в операционном доступе.

125. Физический и логический доступ к оборудованию Удостоверяющего центра разделены процедурно.

126. Для физического доступа к процедурам настройки и обслуживания аппаратных криптографических модулей (Hardware Security Module, HSM) и их ключевого материала требуется участие минимум двоих уполномоченных работников Банка.

127. Процедуры обработки логических запросов к информационной системе Удостоверяющего центра автоматизированы на уровне прикладного программного обеспечения, с контролем полномочий инициаторов запроса.

---

[11] На дату утверждения Политики регистрационных свидетельств действуют Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.

Раздел 5.3. Контроль персонала

128. При назначении на должности работников Удостоверяющего центра и центров регистрации применяются квалификационные требования.

129. Работники Удостоверяющего центра повышают свою квалификацию путем прохождения обучения или сертификации в определенном наборе тем[12].

130. Ограничений на частоту и последовательность перемещений работников Удостоверяющего центра по службе не накладывается, за исключением квалификационных требований к должностям в Удостоверяющем центре.

131. Все функции и работы Удостоверяющего центра выполняются силами штатных работников Банка. Допускается привлечение контрагентов в рамках договоров поставки и технической поддержки аппаратного и программного обеспечения информационной системы Удостоверяющего центра. Привлечение внештатных сотрудников (в форме не трудовых договоров, а договоров гражданско-правового характера) к выполнению функций и работ Удостоверяющего центра не предусмотрено.

132. Каждому работнику Удостоверяющего центра и центров регистрации для компетентного исполнения должностных обязанностей обеспечивается доступ к текстам правовых актов законодательства и внутренних документов Банка.

Раздел 5.4. Процедуры контрольного протоколирования

133. Обработка запросов Удостоверяющим центром осуществляется с обязательным контрольным протоколированием, включающим регистрацию инициатора запроса.

134. В Удостоверяющем центре обязательному протоколированию подлежат следующие типы событий:

1) жизненный цикл криптографических ключей Удостоверяющего Центра (генерация и удаление ключей, создание, хранение, восстановление и уничтожение резервных копий);

2) жизненный цикл регистрационных свидетельств (получение запросов на выпуск и изменение статуса регистрационных свидетельств, генерация и изменение статуса регистрационных свидетельств, генерация и выпуск списков отозванных регистрационных свидетельств);

3) жизненный цикл аппаратных криптографических модулей HSM (получение, ввод в эксплуатацию, штатные процедуры, определенные эксплуатационно-технической документацией, сервисное обслуживание, ремонт, вывод из эксплуатации, уничтожение);

4) жизненный цикл заявлений на выпуск и отзыв регистрационных свидетельств (данные должностного лица, проводившего идентификацию и аутентификацию, дата и время обработки);

5) иные события, подлежащие протоколированию согласно Политике информационной безопасности Банка (сеансы администрирования компонентов информационной системы Удостоверяющего центра, инциденты информационной безопасности и пр.).

135. Криптографические ключи и данные их активации не подлежат записи в контрольные протоколы.

Раздел 5.5. Ведение архива

136. Удостоверяющий центр ведет архив:

1) выпущенных регистрационных свидетельств, включая отозванные регистрационные свидетельства и регистрационные свидетельства с истекшим сроком действия;

2) информации о жизненном цикле регистрационных свидетельств, включая заявления об их выпуске и отзыве, и списки отозванных регистрационных свидетельств;

---

[12] На дату утверждения Политики регистрационных свидетельств действуют Требования к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности, утвержденные постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 21 сентября 2020 года № 89.

3) контрольных протоколов информационной системы (в соответствии с разделом 5.4 Политики регистрационных свидетельств).

137. Архив Удостоверяющего центра ведется на постоянной основе в соответствии с регламентированными сроками и требованиями законодательства Республики Казахстан[13].

138. В случае принятия решения о прекращении деятельности Удостоверяющего центра данные архива подлежат хранению в течение срока, установленного законодательством Республики Казахстан[14].

139. Доступ к архиву предоставляется только работникам Удостоверяющего центра.

140. Внешнее резервирование архива Удостоверяющего центра не предусматривается.

Раздел 5.6. Смена криптографических ключей удостоверяющего центра

141. Новые криптографические ключи Удостоверяющего центра генерируются либо на замену истекающим, либо в дополнение к действующим в целях обеспечения ввода в эксплуатацию новых сервисов.

142. Смена криптографических ключей Удостоверяющего центра осуществляется заблаговременно до истечения срока их действия.

143. Плавность перехода пользователей регистрационных свидетельств (доверяющих сторон) к использованию новых криптографических ключей Удостоверяющего центра обеспечивается за счет выпуска регистрационных свидетельств новых ключей Удостоверяющего центра и прекращения подписания новых регистрационных свидетельств подписчиков теми ключами Удостоверяющего центра, которые подлежат плановой смене. При этом Удостоверяющий центр продолжает подписывать списки отозванных регистрационных свидетельств ключом, срок действия которого завершается, вплоть до того момента, когда истечет срок действия последнего регистрационного свидетельства, подписанного с его помощью.

Раздел 5.7. Восстановление функционирования в случае чрезвычайных происшествий или компрометации

144. На случай чрезвычайных и иных происшествий, влекущих прерывание функционирования сервисов Удостоверяющего центра, составлен План восстановления функционирования Удостоверяющего центра.

145. В Плане восстановления функционирования Удостоверяющего центра предусмотрены:

1) переключение для восстановления на рабочий центр обработки данных;

2) выбор площадки для восстановления на базе основного или резервного центра обработки данных и восстановление рабочих записей из резервной или архивной копии.

146. Приоритетом восстановления функционирования является возобновление основных сервисов Удостоверяющего центра по публикации сведений о статусе регистрационных свидетельств, выпуска и отзыва регистрационных свидетельств.

147. Оборудование Удостоверяющего центра в центрах обработки данных обеспечивается резервированным подключением к сети с использованием нескольких каналов.

148. Все изменения в базах данных Удостоверяющего центра постоянно реплицируются между центрами обработки данных.

149. Обоснованные подозрения в компрометации закрытых криптографических ключей Удостоверяющего центра обрабатываются как инцидент информационной безопасности критического уровня.

150. Проверка готовности резервного оборудования, резервных и архивных копий данных Удостоверяющего центра осуществляется путем переключения работы информационной системы Удостоверяющего центра между основным и резервным центрами обработки данных не реже одного раза в год с использованием рабочих инструкций, изложенных в Плане восстановления функционирования Удостоверяющего центра.

---

[13] Закон Республики Казахстан “Об электронном документе и электронной цифровой подписи” (статья 16).

[14] Закон Республики Казахстан “Об электронном документе и электронной цифровой подписи” (статья 22).

Раздел 5.8. Прекращение работы удостоверяющего центра

151. В случае принятия решения о прекращение работы Удостоверяющего центра уведомление контрагентов Банка, включая владельцев и пользователей регистрационных свидетельств (подписчиков Удостоверяющего центра и доверяющих сторон), передача и архивное хранение записей Удостоверяющего центра организовываются в соответствии с Законом Республики Казахстан “Об электронном документе и электронной цифровой подписи” (статья 22).

Глава 6. Технический контроль безопасности

Раздел 6.1. Генерация и установка криптографических ключей

152. Генерация криптографических ключей проводится только с помощью средств криптографической защиты информации, криптографическая стойкость которых подтверждена сертификатом соответствия действующему в Республике Казахстан стандарту, который определяет общие технические требования к средствам криптографической защиты информации[15] (далее – Стандарт).

153. Генерация криптографических ключей Удостоверяющего центра проводится только несколькими выделенными для этой цели и предварительно обученными работниками. При этом используются только аппаратные криптографические модули (HSM), которые соответствуют не ниже чем второму уровню безопасности согласно Стандарту.

154. В центрах регистрации закрытые криптографические ключи подписчиков генерируются непосредственно на защищенном носителе ключевой информации, исключающем возможность его разглашения, изменения или несанкционированного использования. Все допустимые исключения из настоящего пункта, при их наличии, должны быть указаны в Регламенте деятельности удостоверяющего центра.

155. Перечень криптографических алгоритмов, для которых предназначены ключи, регистрируемые Удостоверяющим центром, приведен в разделе 6.1 Регламента деятельности удостоверяющего центра.

Раздел 6.2. Защита закрытых криптографических ключей и инженерные контроли криптографических модулей

156. Детальные меры защиты закрытых криптографических ключей Удостоверяющего центра от разглашения, искажения, подмены и несанкционированного использования определены в разделе 6.2 Регламента деятельности удостоверяющего центра, и в Политике регистрационных свидетельств не раскрываются. В настоящем разделе приведен общий обзор этих мер.

157. Для генерации и хранения закрытых криптографических ключей Удостоверяющего центра используются аппаратные криптографические модули (HSM), сертифицированные на соответствие Стандарту не ниже, чем по второму уровню безопасности.

158. Закрытые криптографические ключи Удостоверяющего центра после создания не подлежат депонированию. Вместе с тем, в целях обеспечения возможности восстановления функционирования информационной систем после чрезвычайного происшествия или иного сбоя в работе непосредственно после генерации каждого нового закрытого криптографического ключа Удостоверяющий центр создает и хранит резервную копию всех используемых в текущий момент закрытых криптографических ключей.

159. На этапе хранения резервная копия закрытых ключей Удостоверяющего центра защищена от разглашения, искажения и подмены криптографическими и организационными мерами.

160. Шифрование резервной копии закрытых криптографических ключей Удостоверяющего центра при их (за-)выгрузке (в) из аппаратного(-ый) криптографического(-ий) модуля(-ь) (HSM) осуществляется с созданием (использованием) данных активации в форме секрета, разделенного на части, каждая из которых закрепляется за отдельным

[15] На дату утверждения Политики регистрационных свидетельств действует государственный стандарт Республики Казахстан СТ РК 1073-2007 “Средства криптографической защиты информации. Общие технические требования”.

ответственным лицом (хранителем части секрета), записывается на защищенный носитель информации и защищается персональным паролем.

161. Для выполнения операций с криптографическими ключами Удостоверяющего центра, активированными внутри HSM, требуется участие не менее двоих уполномоченных работников Банка.

162. Вышеуказанные HSM, их комплектующие и детали не подлежат выбытию из Банка или повторному использованию в любом ином качестве.

163. Меры защиты от разглашения, искажения, подмены и несанкционированного использования своих закрытых криптографических ключей и данных их активации на всем протяжении их жизненного цикла, от генерации до уничтожения, владельцы регистрационных свидетельств (подписчики Удостоверяющего центра) принимают самостоятельно, в соответствии с требованиями законодательства и Политики регистрационных свидетельств.

Раздел 6.3. Прочие аспекты управления криптографическими ключами

164. Все открытые ключи, заверенные регистрационным свидетельством, которое когда-либо выпустил Удостоверяющий центр, подлежат архивированию в составе этих регистрационных свидетельств, в соответствии с разделом 5.5 Политики регистрационных свидетельств.

165. Срок действия регистрационного свидетельства Удостоверяющего центра составляет не менее 10 лет и исчисляется с даты и времени его выпуска.

166. Сроки действия регистрационных свидетельств подписчиков в различных информационных системах, обслуживаемых Удостоверяющим центром, составляют 1, 2 или 3 года и устанавливаются нормативно-технической документацией заинтересованной информационной системы Банка.

167. Для непрерывной работы в информационных системах, которые требуют наличия регистрационных свидетельств, выпущенных Удостоверяющим центром, подписчики в соответствии с Политикой регистрационных свидетельств наделены правом запрашивать выпуск новых регистрационных свидетельств на замену регистрационных свидетельств с истекающим сроком действия.

Раздел 6.4. Данные активации

168. Закрытые криптографические ключи подписчиков Удостоверяющего центра используются непосредственно на защищенном носителе ключевой информации, исключающем возможность их разглашения, изменения или несанкционированного использования.

169. Для использования закрытого криптографического ключа владельцу регистрационного свидетельства (подписчику Удостоверяющего центра) необходимо создать и применять данные активации в форме пароля.

Раздел 6.5. Контроль безопасности вычислительных ресурсов

170. Вычислительные ресурсы, программное обеспечение и данные информационной системы Удостоверяющего центра защищаются от несанкционированного доступа в соответствии с Политикой информационной безопасности Банка, и в Политике регистрационных свидетельств не раскрываются. В настоящем разделе приведен общий обзор этих мер.

171. Серверы для подписи регистрационных свидетельств, списков отозванных регистрационных свидетельств, ответов (квитанций) службы OCSP защищаются от несанкционированного доступа.

172. Операционные системы серверов поддерживаются на высоком уровне защиты путем применения рекомендованных пакетов защиты и обновлений, в том числе антивирусных.

173. Количество запущенных на серверах служб операционных систем сведено до необходимого минимума.

174. Доступ к администрированию основных серверов разрешен только работникам Удостоверяющего центра, остальные пользователи программных приложений Удостоверяющего центра не имеют доступа к системным или технологическим учетным

записям.

175. Сегменты сети, используемые для обслуживания участников инфраструктуры открытых ключей, логически отделены от остальной сети Банка. Это выделение исключает любой сетевой доступ пользователей к данным Удостоверяющего центра кроме доступа через определенные прикладные программные процессы. Прямой доступ к базам данных Удостоверяющего центра ограничен минимально необходимой группой администраторов информационной системы.

176. Для защиты сегментов сети Удостоверяющего центра от внешнего или внутреннего вмешательства, ограничения содержания и источников сетевой активности используются межсетевые экраны.

177. В деятельности Удостоверяющего центра используются средства криптографической защиты информации (СКЗИ: HSM и программные СКЗИ), сертифицированные на соответствие требованиям Стандарта.

178. Специальных требований по сертификации информационной безопасности иных (некриптографических) компонентов и программного обеспечения не выдвигается.

Раздел 6.6. Контроль управления развитием и безопасностью

179. Работоспособность и целостность технических и программных средств Удостоверяющего центра обеспечивается системой организационных и технических мер, основанных на разделении прав и ответственности за использование этих средств, прав доступа к ним, и техническим средствам ИТ-архитектуры, обеспечивающей доступ.

180. В целях апробации любых изменений в информационной системе Удостоверяющий центр имеет и поддерживает ее тестовый контур, обеспеченный необходимым минимумом вычислительной техники, средств криптографической защиты информации и лицензий на использование программного обеспечения.

Раздел 6.7. Контроль безопасности сети

181. Функции Удостоверяющего центра выполняются в корпоративной сети Банка, защищенной (в регламентированном порядке) от несанкционированного доступа и вмешательства.

Раздел 6.8. Метки времени

182. Регистрационные свидетельства, списки отозванных регистрационных свидетельств, ответы квитанции (ответы службы) OCSP, контрольные протоколы информационной системы Удостоверяющего центра, содержащие информацию о выпуске и изменении статуса регистрационных свидетельств, содержат информацию о дате и времени событий.

Глава 7. Профили регистрационных свидетельств, CORC и OCSP

Раздел 7.1. Профили регистрационных свидетельств

183. Удостоверяющий центр выпускает регистрационные свидетельства в соответствии со стандартом ITU-T X.509.

184. Основные поля, содержащиеся в регистрационных свидетельствах, вместе с требованиями к их содержанию определяются в соответствии с разделом 7.1 Регламента деятельности удостоверяющего центра.

Раздел 7.2. Профили списка отозванных регистрационных свидетельств

185. Удостоверяющий центр выпускает списки отозванных регистрационных свидетельств в соответствии со стандартом ITU-T X.509.

186. Основные поля и расширения, содержащиеся в списках отозванных регистрационных свидетельств, вместе с требованиями к их содержанию определяются в соответствии с разделом 7.2 Регламента деятельности удостоверяющего центра.

Раздел 7.3. Профиль сервиса OCSP

187. Сервис OCSP для получения информации о статусе регистрационных свидетельств, выпущенных Удостоверяющим центром, предоставляется в соответствии с рекомендациями RFC 2560 “X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP” (Онлайн протокол статуса сертификатов интернет инфраструктуры открытых ключей X.509).

Глава 8. Проверка деятельности

188. Деятельность Удостоверяющего центра подлежит регулярным проверкам уполномоченного государственного органа в сфере обеспечения информационной безопасности в процессе аккредитации.

Глава 9. Прочие вопросы

Раздел 9.1. Тарифы

189. Услуги удостоверяющего центра не тарифицируются и не оплачиваются.

Раздел 9.2. Ответственность

190. Ответственность участников инфраструктуры открытых ключей, обслуживаемой Удостоверяющим центром, установлена законодательством Республики Казахстан[16].

Раздел 9.3. Конфиденциальность

191. Регистрационные свидетельства, выпускаемые Удостоверяющим центром, и информация об их отзыве или ином статусе, не являются и не рассматриваются в качестве конфиденциальной информации.

Раздел 9.4. Защита персональных данных участников

192. Любой владелец регистрационного свидетельства (подписчик Удостоверяющего центра) признает, что, подавая заявление на выпуск регистрационного свидетельства в Удостоверяющий центр, он дает согласие на размещение содержащейся в нем информации о себе в публичном доступе. Заявление на выпуск регистрационного свидетельства является письменным документом, означающим согласие субъекта на сбор и обработку его персональных данных в соответствии с законодательством Республики Казахстан по вопросам персональных данных и их защиты[17].

Раздел 9.5. Права интеллектуальной собственности

193. В своей деятельности Удостоверяющий центр использует программное обеспечение, авторские и исключительные имущественные права на которое не принадлежат Банку. Порядок использования программного обеспечения определяется условиями лицензий, приобретенных Банком.

194. Владельцы регистрационных свидетельств (подписчики Удостоверяющего центра) сохраняют все свои права на имена и торговые марки, содержащиеся в регистрационных свидетельствах.

Раздел 9.6. Гарантии и заверения

195. Каждый владелец регистрационного свидетельства (подписчик Удостоверяющего центра) обеспечивает:

1) использование только того своего закрытого криптографического ключа, для которого имеется соответствующее ему регистрационное свидетельство, выпущенное Удостоверяющим центром, принятое владельцем и действительное на момент использования (не просрочено и не отозвано);

2) защиту своих закрытых криптографических ключей от доступа любых других лиц;

---

[16] Кодекс Республики Казахстан “Об административных правонарушениях”, статья 640.

[17] Закон Республики Казахстан “О персональных данных и их защите”, статья 8.

3) достоверность сведений о себе, предоставляемых для выпуска регистрационных свидетельств в центр регистрации;

4) проверку достоверности сведений о себе, содержащихся в регистрационных свидетельствах, перед принятием регистрационного свидетельства;

5) не использование своего закрытого ключа в целях подписания каких-либо регистрационных свидетельств, списков отозванных регистрационных свидетельств, любого другого формата удостоверений открытого ключа или информации о его статусе.

196. Каждый владелец и каждый пользователь регистрационного свидетельства (подписчик Удостоверяющего центра и доверяющая сторона) обеспечивает при использовании регистрационных свидетельств, выпущенных Удостоверяющим центром, принятие только обоснованных решений, опирающихся на достаточный объем объективной информации о регистрационном свидетельстве и его владельце.

Раздел 9.7. Отказ от гарантий

197. Удостоверяющий центр не несет перед владельцами и пользователями регистрационных свидетельств (подписчиками Удостоверяющего центра и доверяющими сторонами) дополнительной ответственности, вытекающей из договоров оказания банковских услуг, включая ответственность за товарную пригодность и соответствие, кроме той ответственности, которая установлена законодательством Республики Казахстан по вопросам электронного документа и электронной цифровой подписи и задекларирована Политикой регистрационных свидетельств.

Раздел 9.8 Ограничение ответственности

198. Ответственность Удостоверяющего центра, центров регистрации, владельцев и пользователей регистрационных свидетельств (подписчиков Удостоверяющего центра и доверяющих сторон) ограничена законодательством Республики Казахстан[18].

Раздел 9.9. Компенсации

199. В части, не противоречащей действующему законодательству Республики Казахстан, на счет владельцев регистрационных свидетельств (подписчиков Удостоверяющего центра) относятся расходы, связанные с компенсацией:

1) предоставления ошибочной, вводящей в заблуждение или заведомо ложной информации в заявлении на выпуск или отзыв регистрационного свидетельства;

2) непреднамеренного или умышленного сокрытия существенных фактов, подлежащих отражению в заявлении на выпуск или отзыв регистрационного свидетельства;

3) непринятия мер защиты собственного закрытого криптографического ключа, приведшее к его компрометации, разглашению, изменению или несанкционированному использованию;

4) использования в составе своего выделенного имени названий, нарушающих права интеллектуальной собственности третьих лиц.

200. В части, не противоречащей действующему законодательству Республики Казахстан, на счет пользователей регистрационных свидетельств (доверяющих сторон) относятся расходы, связанные с компенсацией:

1) необоснованного доверия к регистрационному свидетельству, допущенному из-за нарушения обязательств пользователя регистрационных свидетельств (доверяющей стороны);

2) непринятия мер по проверке регистрационного свидетельства с целью определения его сроков действия и статуса (отозвано/не отозвано).

Раздел 9.10. Вступление в силу и прекращение действия

201. Политика регистрационных свидетельств и все изменения и дополнения к ней вступают в силу со дня опубликования на официальном ресурсе Банка в сети Интернет.

202. Политика регистрационных свидетельств, с учетом публикуемых изменений и

[18] Кодекс Республики Казахстан “Об административных правонарушениях”, статья 640.

дополнений к ней, сохраняет силу до момента опубликования новой редакции Политики регистрационных свидетельств на официальном ресурсе Банка в сети Интернет.

Раздел 9.11. Уведомления и связь с участниками

203. Участники инфраструктуры открытых ключей: Удостоверяющий центр, центры регистрации, владельцы и пользователи регистрационных свидетельств (подписчики Удостоверяющего центра и доверяющие стороны), для связи друг с другом используют любые целесообразные каналы, соответствующие предмету взаимодействия, степени важности и срочности коммуникации, если иное не определено соглашением между сторонами.

Раздел 9.12. Изменения и дополнения

204. Незначительные изменения в Политику регистрационных свидетельств (изменение адресов и ссылок, контактной информации, исправление опечаток и пр.) вносятся без предварительного уведомления участников инфраструктуры открытых ключей. Решения об уровне значимости изменений и дополнений (существенные или несущественные) принимаются Удостоверяющим центром самостоятельно.

205. Существенные изменения и дополнения в Политику регистрационных свидетельств Удостоверяющий центр предварительно публикует, в форме проекта, на официальном информационном ресурсе Банка в сети Интернет, как правило за 14 календарных дней до вступления в силу, если иное не предусмотрено опубликованными изменениями в законодательстве Республики Казахстан.

206. В случае внесения изменений и дополнений в Политику регистрационных свидетельств Удостоверяющий центр отвечает за определение необходимости внесения изменений и дополнений в перечень объектных идентификаторов политики регистрационных свидетельств и приведение его в соответствие с новой редакцией Политики регистрационных свидетельств.

207. Если в связи с изменениями и дополнениями в Политике регистрационных свидетельств необходимо изменение перечня объектных идентификаторов политики регистрационных свидетельств, то соответствующие изменения в него, а также в Регламент деятельности удостоверяющего центра публикуются и вносятся одновременно.

Раздел 9.13. Разрешение споров

208. Споры между участниками инфраструктуры открытых ключей: между владельцами и пользователями регистрационных свидетельств (подписчиками Удостоверяющего центра и доверяющими сторонами), а также между подписчиком или доверяющей стороной с одной стороны, и Удостоверяющим центром или центром регистрации, с другой стороны, - разрешаются в соответствии с положениями договоров, действующих между сторонами, и/или законодательства Республики Казахстан.

209. Если спор не решен в досудебном порядке, то он подлежит разрешению в судебном порядке.

Раздел 9.14. Юрисдикция

210. Для разрешения споров, предметом которых являются разногласия по существу Политики регистрационных свидетельств, применяется законодательство Республики Казахстан.

Раздел 9.15. Соответствие применимому законодательству

211. К участникам инфраструктуры открытых ключей: Удостоверяющему центру, центрам регистрации, владельцам и пользователям регистрационных свидетельств (подписчикам Удостоверяющего центра и доверяющим сторонам), - применимы требования законодательства Республики Казахстан по вопросам:

1) электронного документа и электронной цифровой подписи;
2) разрешений и уведомлений (в части, касающейся реализации СКЗИ);
3) платежей и платежных систем;

4) персональных данных и их защиты.

Раздел 9.16. Прочие положения

212. В случае если часть положений Политики регистрационных свидетельств будет признана неприменимой судом или уполномоченным государственным органом, остальная их часть сохраняет силу.

213. В случае наступления обстоятельств непреодолимой силы (форс-мажор) участники инфраструктуры открытых ключей: Удостоверяющий центр, центры регистрации, владельцы и пользователи регистрационных свидетельств (подписчики Удостоверяющего центра и доверяющие стороны), - руководствуются соответствующими положениями действующих между ними договоров (при наличии).