АО «Jusan Bank»

ПРАВИЛА
деятельности Удостоверяющего центра

Владелец:	Департамент цифрового развития	
Совладелец:		
Разработчик:	Департамент цифрового развития	
Субъекты регулирования:	Департамент технологических решений Департамент сопровождения ИС Департамент архитектурных решений Департамент системного обеспечения и телекоммуникаций Департамент защиты информационных систем	
Утвержден:	Правлением (протокол № 61-23)	от «02» июня 2023г.
ВД, признаваемые утратившими силу:	Правила деятельности Удостоверяющего центра	Утверждены Правлением АО «Jusan Bank» (протокол № 43-23 от 21.04.2023г.)

Содержание

Глава 1. Общие положения

1. Настоящие Правила деятельности удостоверяющего центра (далее – Правила) разработаны в целях обеспечения функционирования удостоверяющего центра АО «Jusan Bank» (далее – УЦ) и оказания услуг по выдаче регистрационного свидетельства физическим лицам - клиентам Банка на основании законодательства Республики Казахстан (далее – РК) по вопросам электронного документа[1] и электронной цифровой подписи и определяют порядок его функционирования.

2. Правила разработаны 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. Правила регулируют меры, реализуемые УЦ при обеспечении набора сервисов, который определен Политикой применения регистрационных свидетельств удостоверяющего центра АО «Jusan Bank» (далее – Политика регистрационных свидетельств/Политика) и включает в себя, но не ограничивается выпуском, управлением и отзывом регистрационного свидетельства.

4. Правила, в отличие от Политики, определяют порядок и процедуры:

1) выполнения функции (работы сервисов) УЦ;

2) обеспечения безопасности и управления ядром инфраструктуры открытых ключей.

5. С момента подписания участником информационной системы, использующей сервисы УЦ, заявления на выпуск регистрационного свидетельства (далее – заявление), для участника становятся обязательными к выполнению применимые к нему требования настоящими Правилами, ссылка на которые содержится в подписанном заявлении.

6. Правила также определяют процедуры проверки, связанные с выпуском и дальнейшим обслуживанием регистрационного свидетельства, которые выпускает УЦ.

7. Регистрационное свидетельство УЦ применимо для следующих целей:

1) подписание электронных документов (кредитных договоров/заявлений) электронной цифровой подписью;
2) проверка электронной цифровой подписи;
3) аутентификация пользователей.

8. Способы использования регистрационных свидетельств УЦ не должны противоречить действующему законодательству РК и требованиям Правил.

9. Перечень видов регистрационных свидетельств, выпускаемых УЦ, с указанием идентифицирующих их признаков (профилей) приведен в нижеследующей таблице:

Описание	**Значение расширения keyUsage**
Регистрационные свидетельства для обеспечения подлинности, целостности и доказательности электронных документов с помощью электронной цифровой подписи	c0 (в соответствии с OID 2.5.29.15)
Регистрационные свидетельства для обеспечения конфиденциальности ключей и данных с помощью шифрования	38 (в соответствии с OID 2.5.29.15)

10. УЦ выпускает регистрационное свидетельство, которое имеет назначение, соответствующее настоящей главе Правил, и, соответственно, разные профили, которые отражаются в расширении "keyUsage" и/или "extendedKeyUsage" регистрационного свидетельства.

[1] Законодательство РК, в том числе Закон РК об электронном документе и электронной цифровой подписи; Закон РК о персональных данных и их защите; Правила создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре, утвержденные Приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НҚ; Правила проверки подлинности электронной цифровой подписи, утвержденные Приказом Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187

11. Область допустимого применения, выпускаемого УЦ регистрационного свидетельства может дополнительно подразделяться с помощью объектных идентификаторов политики, которые фиксируются в расширении регистрационного свидетельства «cerificatePolicies».

12. Объектный идентификатор политики включает следующих работников УЦ:

1) Администратор УЦ – работник Департамента сопровождения ИС, выполняющий функции: разработки шаблонов (настройка конфигурации в приложении по требованию бизнес владельца УЦ), перевыпуск регистрационного свидетельства, проверки работы центра сертификации, обеспечивающий работоспособность центра сертификации;

2) Системный администратор УЦ - работник Департамента системного обеспечения и телекоммуникаций, выполняющий функции, контролирующие/обслуживающие/выполняющие: консоль, сеть, базу данных, сопровождение запуска HSM, обеспечение отказоустойчивости в рамках компетенции, предоставление доступов к серверам УЦ, бэкап HSM;

3) Офицер безопасности УЦ - работник Департамента защиты информационных систем, выполняющий функции хранения токенов;

4) Начальник УЦ – бизнес-владелец УЦ, работник Департамента цифрового развития, выполняющий функции разработки Правила, Политики, приказов, согласование предоставления доступов работникам Банка, разбор конфликтных ситуаций;

5) Дежурный УЦ - работник Департамента системного обеспечения и телекоммуникаций, выполняющий функции по мониторингу центра сертификации/программного обеспечения УЦ.

13. Полный перечень объектных идентификаторов политики в клиентском регистрационном свидетельстве приведен на официальном информационном ресурсе Банка (корпоративный интернет ресурс).

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

15. Наличие объектных идентификаторов политики дает информационным системам, использующим регистрационное свидетельство, возможность дополнительной защиты в форме контроля системой наборов необходимых и запрещенных политик с ограничением применения неподходящего регистрационного свидетельства.

Глава 2. Глоссарий

16. В Правилах используются следующие основные понятия, определения и сокращения:

1) аутентификация – способ проверки подлинности пользователя при помощи комбинации различных параметров, в том числе генерации и ввода паролей или аутентификационных признаков (цифровых сертификатов, токенов, смарт-карт, генераторов одноразовых паролей и средств биометрической идентификации);

2) Банк – АО «Jusan Bank»;

3) бизнес-владелец УЦ – подразделение Банка, являющееся владельцем основного бизнес-процесса УЦ по выпуску регистрационного свидетельства;

4) бизнес-владелец ИС – подразделение Банка, являющееся владельцем бизнес-процесса фронтальной системы Банка (мобильное приложение Jusan, Jusan Business и другие)/центра регистрации. При необходимости внесения изменений/доработок в центр регистрации бизнес-владелец ИС обращается в подразделение Банка, ответственное за техническое сопровождение данной системы, в соответствии с ВД, регламентирующим порядок взаимодействия при разработке, доработке и внедрении информационных систем, подсистем, модулей;

5) блокчейн – информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе данных на базе цепочки

взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования;

6) ВД – внутренние документы Банка;

7) владелец регистрационного свидетельства – физическое лицо, на имя которого выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве;

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

9) доверяющая сторона – пользователь регистрационного свидетельства, использующий полученные сведения о регистрационном свидетельстве, выпущенном УЦ, для проверки принадлежности ЭЦП владельцу посредством корневого УЦ РК, портала Банка, государственных информационных систем, использующие регистрационные свидетельства УЦ;

10) 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;

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

12) идентификация – в контексте Правил, процесс (или результат процесса), который устанавливает идентичность физического лица (показывающий, что данное лицо является однозначно определенным, реально существующим лицом), и состоит из двух этапов:

а) установление соответствия предъявленного лицом имени реально существующей идентичности лица;

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

13) инфраструктура открытых ключей (ИОК) – набор средств (технических, материальных, людских и прочих), 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;

14) информационная система (ИС) – центр регистрации, организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

15) компрометация закрытых ключей – утрата владельцем закрытых ключей уверенности в том, что конкретные закрытые ключи обеспечивают безопасность защищаемой с их помощью информации;

16) носитель ключевой информации – специализированный носитель, в котором для защиты хранящихся закрытых ключей электронной цифровой подписи используется средства криптографической защиты информации, имеющее сертификат соответствия требованиям законодательства РК;

17) объектный идентификатор – уникальный набор цифр, который связан с объектом и однозначно идентифицирует его в мировом адресном пространстве объектов;

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

19) хэш – преобразование массива входных данных произвольной длины в битовую сторону фиксированной длины;

20) Политика применения регистрационных свидетельств (также именуется Политикой регистрационных свидетельств/Политика) – ВД, который представляет собой озаглавленный набор правил, определяющих применимость регистрационного свидетельства в определенной общности (классе) приложений с общими требованиями информационной безопасности;

21) Правила деятельности удостоверяющего центра (Правила) – ВД, который определяет порядок организации основной деятельности УЦ, осуществляемой в соответствии с Политикой, включая течение основных процессов УЦ;

22) регистрационное свидетельство – электронный документ, выдаваемый УЦ для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом РК «Об электронном документе и электронной цифровой подписи»;

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

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

25) средства электронной цифровой подписи (средства ЭЦП) – совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи (средства электронной цифровой подписи являются одной из разновидностей средств криптографической защиты информации);

26) токен – в контексте Правил, физическое устройство, выдаваемое уполномоченному лицу в целях организации защищенного хранения резервной копии закрытых ключей и настроек аппаратных криптографических модулей (Hardware Security Module, HSM) УЦ;

27) участники инфраструктуры открытых ключей (участники ИОК) – работники УЦ, ответственные за обслуживание клиентов, а также владельцы регистрационного свидетельства;

28) Удостоверяющий центр (УЦ) – Банк, удостоверяющий соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающий достоверность регистрационного свидетельства;

29) центр сертификации – программно-аппаратный комплекс УЦ для выдачи, обслуживания и отзыва регистрационного свидетельства, своевременный импорт СОРС, действующий в соответствии с законодательством РК. При недоступности сервиса центра сертификации выпуск регистрационных свидетельств УЦ не осуществляется;

30) центр регистрации – фронтальная система Банка (мобильное приложение Jusan), принимающая заявления от владельца на выпуск и отзыв регистрационного свидетельства, а также осуществляющая проверку, идентификацию и аутентификацию заявителей. При недоступности сервиса центра регистрации выпуск и отзыв регистрационных свидетельств УЦ не осуществляется;

31) 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 ключа лицу, указанному в заключительном регистрационном свидетельстве последовательности, в поле «subject»;

32) электронная цифровая подпись (ЭЦП) – набор электронных цифровых символов,

созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

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

Иные термины и сокращения, используемые по тексту Правил, применяются в соответствии со значением, закрепленным в законодательстве РК, общебанковском глоссарии, а при их отсутствии в законодательстве РК и общебанковском глоссарии – в соответствии со значением, закрепленном в международной банковской практике.

Все ссылки на части, разделы, главы, параграфы, пункты, приложения в тексте Правил без указания названия документа относятся к настоящим Правилам.

Глава 3. Хранилище и публикация данных (регистрационного свидетельства)

§1. Хранилище

17. УЦ на официальном информационном ресурсе Банка (корпоративный интернет ресурс) с целью уведомления владельцев и доверяющих сторон о выпуске регистрационного свидетельства и размещения СОРС, а также в соответствии с Политикой публикует:

1) Политику регистрационных свидетельств;

2) Правила;

3) регистрационные свидетельства УЦ;

4) ссылки для доступа к СОРС.

18. Официальным уведомлением УЦ владельцев и доверяющих сторон о выпуске регистрационного свидетельства и размещения СОРС является публикация в хранилище, которая доступна через корпоративный интернет ресурс Банка, а также сохранение его в центре регистрации. Дополнительно корпоративный интернет ресурс Банка используется для размещения иной важной информации УЦ, в целях уведомления владельцев и пользователей регистрационных свидетельств (владельцев и доверяющих сторон).

§2. Публикация в хранилище информации о регистрационных свидетельствах

19. Основным протоколом информационного взаимодействия с хранилищем УЦ является облегченный протокол доступа к каталогам в версии, определенной рекомендациями RFC 2251 (Lightweight Directory Access Protocol v.3, версия 3).

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

21. Любые исключения из этих требований, в случае их возникновения, должны быть включены в Правилах и опубликованы в свободном доступе владельцев и пользователей регистрационных свидетельств (владельцев и доверяющих сторон).

22. В хранилище УЦ в режиме онлайн публикуются все действующие регистрационные свидетельства (валидные регистрационные свидетельства, не имеющие статуса «отозвано»), а также СОРС.

§3. Периодичность актуализации данных в хранилище

23. Каждое регистрационное свидетельство, выпущенное УЦ, вносятся в хранилище и публикуется автоматически и немедленно (в режиме онлайн).

24. Начало периода действия закрытого ключа владельца исчисляется с даты и времени начала действия соответствующего регистрационного свидетельства.

25. Срок действия регистрационных свидетельств УЦ:

1) корневого регистрационного свидетельства – 20 (двадцать) лет с момента его выдачи;

2) регистрационного свидетельства, закрытые ключи которого хранятся в УЦ - 1 (один) год с момента его выдачи.

26. Проверка истечения срока действия всех регистрационных свидетельств, размещенных в хранилище, осуществляется автоматически ежесуточно по расписанию, определенному соответствующей настройкой ИС УЦ.

27. При отзыве УЦ регистрационное свидетельство автоматически удаляется из хранилища и переносится в архив, где хранится в соответствии с требованиями законодательства РК.

28. Регистрационные свидетельства, которые не были отозваны, но прекратили действие в связи с истечением срока действия, автоматически удаляется из хранилища и переносится в архив.

29. Сведения об отозванных регистрационных свидетельствах с истекшим сроком действия удаляются из списков отозванных регистрационных свидетельств по факту истечения срока действия регистрационного свидетельства, не реже одного раза в неделю по расписанию, определенному соответствующей настройкой центра сертификации.

30. В случае отзыва любого регистрационного свидетельства УЦ автоматически и немедленно в режиме онлайн формирует и публикует в хранилище обновленный СОРС.

31. В условиях отсутствия событий отзыва регистрационных свидетельств, новый СОРС формируются и выпускаются автоматически на еженедельной основе по расписанию, определенному соответствующей настройкой центра сертификации.

32. Срок хранения отозванных регистрационных свидетельств в хранилище составляет не менее 5 (пяти) лет. По истечении срока отозванные регистрационные свидетельства поступают в архив.

§4. Контроль доступа к хранилищу

33. Доступ для чтения данных из хранилища предоставляется УЦ к обслуживаемым ИС Банка, по заявкам, в порядке, установленном ВД о правилах монтажа и размещения систем контроля и управления доступом.

34. Доступ для добавления, изменения (удаления) данных в(из) хранилище(-а) предоставляется УЦ для ограниченного круга уполномоченных лиц: Администратору УЦ, Системному администратору УЦ согласно матрице доступов.

35. УЦ осуществляет защиту от несанкционированного доступа к хранилищу. Сведения, публикуемые на корпоративном интернет ресурсе Банка, предоставляются участникам ИОК в режиме свободного доступа с правами «только для чтения».

36. В случаях превышения нагрузки на сервис доступа в хранилище соответствующих параметров уровня обслуживания УЦ автоматически применяет временные ограничения доступа в качестве активных мер противодействия кибератакам, иным угрозам перебоя в предоставлении сервисов.

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

Глава 4. Идентификация и аутентификация владельцев регистрационных свидетельств

§1. Требования к именам

38. Используемые УЦ правила именования субъектов обеспечивают идентификацию владельцев регистрационных свидетельств (владельцев) по всем выпускаемым регистрационным свидетельствам.

39. Идентификации владельцев-резидентов регистрационных свидетельств достигается за счет использования идентификационных номеров (ИИН).

40. Идентификация физического лица-нерезидента достигается за счет номера и других данных паспорта.

41. Анонимность владельцев регистрационных свидетельств не допускается.

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

43. Заявители на выпуск регистрационного свидетельства не должны использовать в своих заявлениях имена, нарушающие права их законных правообладателей.

44. Центр регистрации оставляет за собой право отклонить любое заявление на выпуск регистрационного свидетельства, если ему становится известно о факте предоставления недостоверной информации.

45. Во всех без исключения регистрационных свидетельствах, выпускаемых УЦ, имена субъектов указываются в формате выделенных имен (DN-имен) в полях «Issuer» и «Subject» в соответствии с международными рекомендациями ITU-T X.520.

46. Атрибуты и содержание полей «Issuer» и «Subject» корневого регистрационного свидетельства УЦ приведены в нижеследующей таблице:

Атрибут	**Значение**
Country (C=)	KZ
Organization (O=)	Jusan Bank JSC
Common Name (CN=)	Certification Authority

47. В корневом регистрационном свидетельстве УЦ в поле «Subject» содержатся в точности те же данные, что и в поле «Issuer».

48. В поле “Issuer” всех некорневых регистрационных свидетельств, выпускаемых УЦ, включаются в точности те же атрибуты и те же значения, что и в поле «Issuer» корневого регистрационного свидетельства.

49. В регистрационные свидетельства владельцев в поле «Subject» включается набор атрибутов, который приведен в нижеследующей таблице:

Атрибут	**Значение**
Country (C=)	KZ
Organization (O=)	Jusan Bank JSC
Organization unit (OU=)	*Логическая или структурная единица Банка, например, информационная система Банка, ее подсистема, блок, департамент или иное подразделение Банка*
Common name (CN=)	*Код владельца регистрационного свидетельства (ФИО)*
Unique identification number (UID=)	*Код владельца регистрационного свидетельства (ИИН)*

50. Для целей однозначной идентификации, имена всех владельцев регистрационных свидетельств являются уникальными.

§2. Первоначальная проверка идентичности владельца

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

52. Центр регистрации проводит первоначальную проверку идентичности владельца в соответствии с правовым актом РК по вопросам выдачи, хранения, отзыва регистрационных свидетельств, изданным уполномоченным органом в сфере информатизации (далее – Правовой акт регулятора)[2].

[2] Правила выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром, за исключением корневого удостоверяющего центра Республики Казахстан, удостоверяющего центра государственных органов, национального удостоверяющего центра Республики Казахстан и доверенной третьей стороны Республики Казахстан, утвержденные Приказом Министра по инвестициям и развитию Республики Казахстан от 23 декабря 2015 года № 1231

53. Подтверждение принадлежности и действительности открытого ключа ЭЦП УЦ осуществляется участником ИОК/ ИС при обмене электронными документами между участниками ИОК.

54. Участник ИОК/ИС при получении электронного документа, содержащего регистрационные свидетельства подписывающей стороны, осуществляет его проверку на подтверждение принадлежности и действительности открытого ключа ЭЦП путем:

1) проверки регистрационного свидетельства подписывающей стороны;

2) проверки ЭЦП в электронном документе.

Глава 5. Операционные требования к жизненному циклу регистрационных свидетельств

§1. Заявления на выпуск (выдачу) регистрационного свидетельства

55. Центр регистрации принимает заявление на выпуск регистрационного свидетельства от физических лиц, действующих самостоятельно.

56. Заявление заявителя на выпуск (выдачу) регистрационного свидетельства подается в центре регистрации по форме, согласно Правовому акту регулятора.

57. Выдача регистрационного свидетельства владельцу осуществляется центром регистрации.

58. Регистрационное свидетельство владельца, выдаваемое УЦ и регистрационное свидетельство УЦ должны соответствовать требованиям стандарта X.509 и рекомендациям стандарта RFC 5280.

59. Выдача регистрационного свидетельства заявителю осуществляется в форме электронного документа, со структурой регистрационного свидетельства, по форме согласно Правовому акту регулятора.

60. УЦ включает свое имя в каждое выпущенное им регистрационное свидетельство, CORC и подписывает их при помощи собственного закрытого ключа ЭЦП.

61. При выдаче регистрационных свидетельств данное регистрационное свидетельство подписывается ЭЦП УЦ.

62. Заявление на выпуск регистрационного свидетельства содержит ссылку на Политику и Правила.

63. Заявление на выпуск регистрационного свидетельства является документом, означающим принятие заявителем обязательств владельца и пользователя регистрационных свидетельств (владельца и доверяющей стороны) соблюдать принципы и выполнять требования Политики и Правил.

64. Необходимые УЦ обязательства владельца и пользователя регистрационных свидетельств (владельца и доверяющей стороны) изложены в параграфе 4 главы 10 Правил («Гарантии и заверения»).

§2. Обработка заявлений на выпуск регистрационных свидетельств

65. Подача заявления на выпуск регистрационного свидетельства осуществляется через центр регистрации.

66. В процессе запроса заявитель должен:

1) дать согласие на сбор и обработку персональных данных;

2) пройти процедуру аутентификации, включая биометрическую аутентификацию;

3) дать согласие на хранение закрытого ключа облачной ЭЦП в модуле безопасности HSM УЦ. После создания, закрытый ключ ЭЦП сохраняется в HSM в зашифрованном виде. В качестве секретных значений используется пароль, который в УЦ не хранится.

67. УЦ выдает регистрационное свидетельство в случае успешного прохождения заявителем процедур идентификации и аутентификации.

68. Центр регистрации отказывает в приеме документов в день обращения заявителя в случае, если заявитель при подаче заявления в установленный срок не прошел успешно процедуру идентификации и аутентификации.

69. Все зарегистрированные заявления на выпуск регистрационного свидетельства, не отклоненные по указанным основаниям, подлежат удовлетворению в установленный срок.

70. Заявление на выпуск регистрационных свидетельств может быть отклонено центром регистрации в случаях, если:

1) заявитель указал в нем не всю информацию, необходимую в соответствии с Правовым актом регулятора;

2) заявитель указал в них недостоверные сведения;

3) в соответствии со вступившим в законную силу решением суда;

4) заявитель не достиг возраста 16 (шестнадцати) лет;

5) в иных случаях, установленных законодательством РК.

71. В случае изменения, определенного законодательством РК, перечня оснований для отказа в выдаче регистрационного свидетельства применяются требования действующего законодательства РК. Правила подлежат приведению в установленном порядке в соответствии с действующим законодательством РК.

72. Заявления на выпуск регистрационных свидетельств рассматриваются УЦ в общей сложности в срок не более 5 (пяти) рабочих дней с даты регистрации заявления.

§3. Выпуск регистрационного свидетельства

73. Для выпуска регистрационного свидетельства заявителю необходимо пройти следующие этапы:

1) идентификацию личности заявителя;

2) защищенную генерацию ключевой пары в центре сертификации;

3) защищенную доставку открытого ключа заявителю; проверку факта владения закрытым ключом, соответствующим открытому ключу, который подлежит регистрации УЦ.

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

75. Любое регистрационное свидетельство, выпущенное УЦ, автоматически публикуется в хранилище.

76. Защита открытого ключа владельца регистрационного свидетельства от подмены или искажения в случае необходимости его доставки из центра сертификации в центр регистрации достигается за счет использования механизма ЭЦП. Открытый ключ включается в контекст запроса на выпуск регистрационного свидетельства, который составляется в формате PKCS#10 и подписывается закрытым ключом.

77. Фактом владения заявителем закрытым ключом служит наличие ЭЦП в электронном запросе формата PKCS#10, которую выявляет центр сертификации при обработке запроса.

78. При недоступности сервисов центра регистрации, центра сертификации выпуск (выдача) регистрационных свидетельств УЦ не осуществляется.

§4. Использование регистрационного свидетельства и ключевых пар

79. Прежде чем, предпринять любой акт, основываясь на доверии к регистрационному свидетельству, выпущенному УЦ, 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 или COPC.

80. Закрытый ключ используется владельцем регистрационного свидетельства только после того, как он дал письменное обязательство выполнять обязанности владельца и доверяющей стороны в соответствии с Политикой, УЦ выпустил регистрационное свидетельство соответствующего открытого ключа, и владелец принял это регистрационное свидетельство.

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

82. Закрытый ключ используется владельцем только в соответствии с Правовым актом регулятора, договорными обязательствами, Политикой и Правилами.

83. Для проведения проверки ЭЦП пользователь регистрационного свидетельства (доверяющая сторона) выполняет следующие действия:

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. Центр сертификации не предоставляет сервис контроля полномочий.

84. Если один из шагов проверки дает отрицательный результат или его невозможно выполнить, то пользователь (доверяющая сторона) полагает ЭЦП недействительной и отвергает электронный документ.

85. Если в электронном документе имеется отметка времени, сформированная УЦ, то для выполнения действия, требующего доверия к отметке времени, доверяющая сторона также проверяет 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 владельцем до отзыва одного из регистрационных свидетельств цепочки. УЦ 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.

87. Если обстоятельства указывают на необходимости дополнительных гарантий со стороны авторов электронного документа, то пользователь регистрационного свидетельства (доверяющая сторона) получает такие дополнительные гарантии (подтверждающие документы) от владельцев регистрационных свидетельств самостоятельно, до выполнения действий, требующих доверия к регистрационному свидетельству, и без обращения в УЦ.

88. Если пользователь регистрационного свидетельства (доверяющая сторона), предпринимая любой акт, основанный на доверии к регистрационному свидетельству, выпущенному УЦ, не выполнил вышеперечисленные условия Правил, то УЦ не несет перед доверяющей стороной ответственности за последствия такого акта. Услуг по обновлению сроков действия в регистрационных свидетельствах УЦ не предоставляет.

§5. Смена ключей в регистрационном свидетельстве

89. Для смены ключей и при необходимости дальнейшего использования сервисов центра сертификации, требующих наличия ключей, владелец регистрационного свидетельства повторно проходит процедуру выпуска (нового) регистрационного свидетельства, в порядке, определенном Правилами.

90. Смена ключей – подразумевает изготовление нового закрытого ключа и соответствующего ему регистрационного свидетельства. Процедура подачи заявления и выдачи регистрационного свидетельства при смене ключей полностью аналогична

процедурам подачи заявления на выпуск (выдачу) регистрационного свидетельства и его обработки.

91. Замена ключей до истечения срока действия регистрационного свидетельства может быть выполнена при предоставлении запроса, подписанного личным ключом, который соответствует действующему регистрационному свидетельству владельца.

92. При замене ключей в регистрационном свидетельстве по истечению срока действия используется процедура идентификации и аутентификации как при первичном получении регистрационного свидетельства.

93. Для выпуска нового регистрационного свидетельства сначала владелец регистрационного свидетельства подает заявление на отзыв регистрационного свидетельства, а затем заявление на выпуск нового.

§6. Изменение данных в регистрационном свидетельстве

94. Услуг по изменению данных в регистрационном свидетельстве УЦ не предоставляет.

95. Для изменения данных в регистрационном свидетельстве его владелец повторно проходит процедуру выпуска (нового) регистрационного свидетельства, в порядке, определенном Правилами.

96. При этом сначала владелец регистрационного свидетельства подает заявление на отзыв действующего регистрационного свидетельства, а затем заявление на выпуск нового.

§7. Отзыв регистрационных свидетельств

97. Отзыв регистрационного свидетельства осуществляется по заявлению, оформленному владельцем регистрационного свидетельства или УЦ.

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

99. Для отзыва регистрационного свидетельства, владелец регистрационного свидетельства – физическое лицо через центр регистрации подает заявление на отзыв регистрационного свидетельства по форме, согласно Правовому акту регулятора.

100.УЦ отзывает регистрационное свидетельство в следующих случаях:

1) по требованию владельца регистрационного свидетельства;

2) при установлении центром регистрации факта представления недостоверных сведений либо неполного пакета документов при получении регистрационного свидетельства;

3) смерти владельца регистрационного свидетельства;

4) изменения фамилии, имени или отчества (если оно указано в документе, удостоверяющем личность) владельца регистрационного свидетельства;

5) по вступившему в законную силу решению суда.

Удостоверяющий центр производит отзыв регистрационного свидетельства без заявления от заявителя при наступлении одного из случаев, указанных в настоящем пункте, за исключением подпункта 1) настоящего пункта.

101.Отзыв регистрационного свидетельства по требованию владельца регистрационного свидетельства осуществляется в течение одного рабочего дня.

102.В случае изменения, определенного законодательством РК, перечня оснований для отзыва регистрационного свидетельства, применяются требования действующего законодательства РК. Настоящие Правила подлежат приведению в соответствие с законодательством РК в установленном порядке.

103.Центр регистрации обрабатывает заявления на отзыв регистрационного свидетельства, оформленные от владельца регистрационного свидетельства.

104.Перед отзывом регистрационного свидетельства заявитель проходит идентификацию в центре регистрации.

105.Процедура отзыва регистрационного свидетельства осуществляется в соответствии с Правовым актом регулятора и настоящей главой Правил.

106.Доверяющие стороны проверяют статус всех регистрационных свидетельств, на которые они полагаются в своих действиях.

107.Для обеспечения непрерывной возможности проверки статуса регистрационных свидетельств доверяющими сторонами, УЦ:

1) публикует в хранилище обновляемые СОРС согласно главе 3 Правил;

2) обеспечивает функционирование службы протокола OCSP (OCSP – сервис для получения информации о статусе регистрационных свидетельств, выпущенных УЦ (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)).

108.Услуг по временному приостановлению или возобновлению действия регистрационного свидетельства УЦ не предоставляет.

109.Услуг по депонированию закрытого ключа владельца регистрационного свидетельства УЦ не предоставляет.

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

111.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 СОРС, опубликованный в хранилище УЦ.

112.Актуальный СОРС УЦ доступен в корпоративном интернет ресурсе Банка круглосуточно и непрерывно, за исключением времени плановых профилактических работ в соответствии с условиями соглашения об уровне обслуживания УЦ.

113.Исключение истекших регистрационных свидетельств из СОРС осуществляется не реже интервала, определенного соответствующей настройкой центра сертификации.

114.Новый СОРС формируется и публикуется на корпоративном интернет ресурсе Банка: по факту отзыва регистрационного свидетельства любого участника ИОК либо по расписанию, определенному соответствующей настройкой центра сертификации (если в течение установленного периода ни одно регистрационное свидетельство не было отозвано).

115.Вновь созданный СОРС автоматически сохраняется в хранилище УЦ незамедлительно по факту формирования.

116.Владелец регистрационных свидетельств имеет возможность прекратить обслуживание в УЦ:

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

2) отзывая действующее регистрационное свидетельство до окончания срока его действия.

117.В случае истечения срока действия регистрационного свидетельства владельца, обслуживание владельца в УЦ прекращается автоматически.

118.В случае компрометации закрытых ключей УЦ, Администратор УЦ оповещает об этом бизнес-владельцев ИС Банка, использующих сервисы центра сертификации и центра регистрации.

Глава 6. Виды контроля Удостоверяющего центра (физический, операционный, управляющий)

§1. Физический контроль

119.Центр сертификации, обрабатывающий запросы участников ИОК расположен в специализированных центрах обработки данных Банка.

120.Все помещения УЦ оборудованы системой контроля и управления доступом с идентификацией по смарт-картам, исполнительными устройствами системы контроля доступа электромеханического типа в соответствии с:

1) ВД, регламентирующего процедуру организации пропускного и внутриобъектного режима;

2) ВД, регламентирующего порядок монтажа и размещения систем контроля и управления доступом;

3) ВД, регламентирующего порядок монтажа и размещения систем охранного телевидения.

121.Технические средства центра сертификации подключены к общегородской сети электроснабжения с использованием оборудования бесперебойного питания. Электрические сети и электрооборудование, используемые в центре сертификации, отвечают требованиям действующих правил техники безопасности в соответствии с ВД, регламентирующим порядок технического оснащения серверных помещений. Помещения УЦ оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством РК.

122.Защита оборудования центра сертификации от влаги обеспечивается его размещением в специальных серверных шкафах в соответствии с ВД, регламентирующим порядок технического оснащения серверных помещений.

123.Помещение, где расположен центр сертификации оборудовано средствами пожаротушения в соответствии с требованиями, установленными законодательством РК.

124.Документальный архив центра сертификации хранится в соответствии с действующим законодательством РК.

125.Выделенные к уничтожению документы и их уничтожение, не подлежащих архивному хранению, осуществляется работниками УЦ, обеспечивающими документирование. Сменные носители информации физически уничтожаются перед утилизацией.

126.Деятельность центра регистрации ведется только на физически защищенных объектах, в условиях, где затруднены и фиксируются любые попытки несанкционированного доступа, использования или раскрытия конфиденциальной информации в соответствии с:

1) ВД, регламентирующим порядок монтажа и размещения систем контроля и управления доступом;

2) ВД, регламентирующим порядок монтажа и размещения систем охранного телевидения;

3) ВД, регламентирующим процедуру организации пропускного и внутриобъектного режима;

4) ВД, регламентирующим порядок технического оснащения серверных помещений.

127.Центр сертификации обеспечен 2 (двумя) центрами обработки данных (основной и резервный), расположенными на разных объектах, в целях резервирования и восстановления функционирования в случае чрезвычайной ситуации.

128.Физический доступ основного и резервного центра обработки данных организованы и контролируются одинаковыми мерами безопасности, в соответствии с ВД, регламентирующим процедуру организации пропускного и внутриобъектного режима.

129.Серверные помещения центров обработки оборудованы системами:

1) контроля и управления доступом;

2) охранной сигнализации;

3) видеонаблюдения;

4) гарантированного электропитания;

5) электрического заземления;

6) обеспечения микроклимата;

7) пожарной сигнализации;

8) газового автоматического пожаротушения.

130. Подразделения, реализующие меры пропускного и внутриобъектового режима в Банке, являются независимыми от центра сертификации. Контроль процессов, реализующих меры пропускного и внутриобъектового режима в Банке, обеспечивается подразделением безопасности в соответствии с ВД, регламентирующим процедуру организации пропускного и внутриобъектного режимов в Банке и службой внутреннего аудита посредством независимой оценки в соответствии с внутренним документом Банка.

§2. Операционный контроль

131.Центры обработки данных УЦ обеспечиваются круглосуточной технической поддержкой в режиме онлайн 24/7/365, включающей перезагрузку оборудования и замену комплектующих.

132.Требования к уровню услуг центра сертификации со стороны заинтересованных ИС Банка составляют:

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

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

3) обслуживание не менее 4 000 000 (четырех миллионов) регистрационных свидетельств в операционном доступе.

133.По соглашению об уровне обслуживания допустимое время простоя оборудования в центрах обработки данных по причине отказов оборудования и каналов связи составляет не более 18 (восемнадцати) часов в год (99.8% (девяносто девять тысяч восемь десятых процентов)) за исключением плановых работ по модернизации или форс-мажорных обстоятельств, неподконтрольных поставщикам услуг.

134.Время реакции поставщика услуг центров обработки данных – не более 1 (одного) часа с момента оформления заявки центром регистрации.

135.Из всего набора рабочих процедур УЦ особыми организационными мерами выделены процедуры настройки и обслуживания аппаратных криптографических модулей (Hardware Security Module, HSM) и их ключевого материала, в соответствии с ВД, регламентирующим установку и настройку программного обеспечения УЦ.

136.С момента ввода в устройства HSM ключей для физического доступа к HSM и ключам требуется участие минимум 2 (двоих) уполномоченных работников Банка.

137.Работники, осуществляющие операционный контроль работы HSM (Администратор УЦ, Системный администратор УЦ), не работают с ключами физически и наоборот.

§3. Управляющий контроль

138.Перед назначением на должности работников по обслуживанию центра сертификации соискатели предоставляют документы, определенные Трудовым кодексом РК и проходят скрининг в соответствии с ВД, регламентирующие процессы Банка по подбору персонала.

139.Работники и руководители УЦ, связанные с обслуживанием центра сертификации проходят обучение или сертификацию не реже 1 (одного) раза в 3 (три) года для соответствия квалификационным требованиям.

140.Ограничений на частоту и последовательность перемещений работников УЦ, связанных с обслуживанием центра сертификации по службе не накладывается, за исключением квалификационных требований к должностям.

141.Ответственность работников УЦ, обслуживающих центр сертификации за несанкционированный доступ к служебной информации и иные нарушения требований информационной безопасности предусмотрена трудовым договором и должностными инструкциями.

142.Дисциплинарные взыскания по факту нарушения требований информационной безопасности определяются и выносятся приказами в соответствии с ВД, регламентирующим применение дисциплинарных взысканий к работникам Банка.

143.Каждому работнику УЦ обслуживающему центр сертификации для компетентного исполнения должностных обязанностей, обеспечивается доступ к текстам правовых актов законодательства РК и ВД Банка.

§4. Процедуры контрольного протоколирования

144.Структура записи контрольного протокола включает в себя:

1) дату и время записи;

2) порядковый номер записи;

3) идентичность сущности, которая инициировала событие, подлежащее протоколированию;

4) тип события;

5) источник записи.

145.Протоколы событий ежедневно преобразуется в хэш, и данные хэш хранятся в цепочке событий блокчейн. Применяемая для этого блокчейн доступна в интернет.

146.В УЦ обязательному протоколированию подлежат следующие типы событий:

1) жизненный цикл ключей УЦ (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 СОРС);

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 идентификации и аутентификации, дата и время обработки);

5) иные события, подлежащие протоколированию согласно Политике информационной безопасности Банка (сеансы администрирования компонентов ИС УЦ, инциденты информационной безопасности и прочее).

147.Ключи и данные их активации не подлежат записи в контрольные протоколы.

148.Контрольные протоколы УЦ ведутся центром сертификации непрерывно, подлежат ежесуточному резервному копированию, ежемесячному архивированию и сдаче в архив в соответствии с главой 6 Правил, где хранятся в течение 1 (одного) года с даты истечения срока действия регистрационного свидетельства.

149.Документы (заявления и иные подтверждающие документы) владельцев регистрационных свидетельств и контрагентов УЦ регистрируются, систематизируются и хранятся в соответствии с ВД Банка, регулирующие процессы по вопросам делопроизводства.

§5. Смена ключей Удостоверяющего центра

150.Смена ключей УЦ осуществляется заблаговременно до истечения срока их действия.

151.Новые ключи УЦ генерируются либо на замену истекающим, либо в дополнение к действующим в целях обеспечения ввода в эксплуатацию новых сервисов.

152.Плавность перехода пользователей регистрационных свидетельств (доверяющих сторон) к использованию новых ключей УЦ обеспечивается за счет выпуска регистрационных свидетельств новых ключей УЦ и прекращения подписания новых регистрационных свидетельств владельцев теми ключами УЦ, которые подлежат плановой смене. При этом, УЦ продолжает подписывать СОРС ключом, срок действия которого завершается, вплоть до того момента, когда истечет срок действия последнего регистрационного свидетельства, подписанного с его помощью.

153.Заблаговременно, до окончания срока действия закрытого ключа уполномоченного лица УЦ, Администратор УЦ производит формирование нового закрытого ключа и регистрационного свидетельства уполномоченного лица УЦ и публикует его в соответствующий раздел хранилища. По окончании действия закрытого ключа, носители ключевой информации с закрытым ключом и его копиями уничтожаются по акту. Все владельцы и пользователи регистрационных свидетельств обязаны получить новое регистрационное свидетельство УЦ и добавить его в справочники регистрационных свидетельств без удаления действующего регистрационного свидетельства УЦ.

§6. Восстановление функционирования в случае чрезвычайных происшествий или компрометации

154.В случае чрезвычайных происшествий, влекущих прерывание функционирования сервисов УЦ, выполняются действия в соответствии с Инструкцией по действиям работников Удостоверяющего центра во внештатных, кризисных ситуациях (далее – Инструкция во внештатных, кризисных ситуациях), Инструкцией по резервному копированию, архивированию и восстановлению данных информационных систем Удостоверяющего центра (далее – Инструкция по резервному копированию) и Правилами по обеспечению непрерывной работы активов, связанных со средствами обработки информации (далее – Правила по обеспечению непрерывной работы активов).

155.В Инструкции во внештатных, кризисных ситуациях, Инструкции по резервному копированию и Правилах по обеспечению непрерывной работы активов 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.

156.Резервный центр обработки данных обеспечен запасным оборудованием. Создание и хранение резервных и архивных копий рабочих записей УЦ регламентированы в Инструкции во внештатных, кризисных ситуациях, Инструкции по резервному копированию и Правилами по обеспечению непрерывной работы активов.

157. В случае повреждения вычислительных, программных ресурсов и/или данных информационной системы УЦ обрабатываются в соответствии с Инструкцией во внештатных, кризисных ситуациях и Правилами по обеспечению непрерывной работы активов.

158.В случае принятия УЦ решения об отзыве регистрационного свидетельства УЦ выполняются следующие процедуры:

1) информация об отзыве публикуется в СОРС в соответствии с Правилами;

2) в соответствии с Инструкцией во внештатных, кризисных ситуациях и Правилами по обеспечению непрерывной работы активов предпринимаются иные целесообразные меры для дополнительного уведомления доверяющих сторон об отзыве регистрационного свидетельства УЦ;

3) за исключением случаев прекращения деятельности УЦ генерируются новые ключи в соответствии с Правилами.

159.Актуальность Инструкции во внештатных, кризисных ситуациях, Инструкции по резервному копированию и Правил по обеспечению непрерывной работы активов проверяется по мере внесения изменений в центре сертификации или по результатам переключения центра сертификации между основным и резервным центрами обработки данных, но не реже 1 (одного) раза в год.

160.Оборудование УЦ в центрах обработки данных обеспечивается резервированным подключением к сети с использованием нескольких каналов.

161. Все изменения в базах данных УЦ постоянно реплицируются между центрами обработки данных.

162. Обоснованные подозрения в компрометации закрытых ключей УЦ обрабатываются как инцидент информационной безопасности критического уровня.

163. Проверка готовности резервного оборудования, резервных и архивных копий данных УЦ осуществляется путем переключения работы центра сертификации между основным и резервным центрами обработки данных не реже 1 (одного) раза в год с использованием Инструкции по резервному копированию, Инструкции во внештатных, кризисных ситуациях и Правил по обеспечению непрерывной работы активов.

164. В случае принятия решения о прекращение работы УЦ уведомление контрагентов Банка, включая владельцев и пользователей регистрационных свидетельств (владельцев и доверяющих сторон), передача и архивное хранение записей УЦ организовываются в соответствии с Законом РК «Об электронном документе и электронной цифровой подписи».

§7. Ведение архива

165.УЦ 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 СОРС;

3) контрольных протоколов информационной системы.

166.Хранение носителей архивной информации, маркировка архивных носителей информации, защита данных архива от несанкционированного просмотра, изменения и удаления осуществляются в соответствии с Инструкцией по эксплуатации магнитных лент системы резервного копирования и жестких дисков серверного оборудования и систем хранения данных.

167.Утилизация носителей конфиденциальных данных УЦ осуществляется в соответствии с Инструкцией по эксплуатации магнитных лент системы резервного копирования и жестких дисков серверного оборудования и систем хранения данных.

168.В случае принятия решения о прекращении деятельности УЦ данные архива подлежат хранению в течение срока, установленного законодательством РК.

169. Доступ к архиву предоставляется только работникам УЦ обслуживающим центр сертификации.

170.Внешнее резервирование архива центра сертификации не предусматривается.

Глава 7. Технический контроль безопасности

§1. Генерация и установка ключей

171.По каждому факту генерации ключей центром сертификации составляется протокол, который датируется и подписывается лицами, принимавшими участие в процедуре. Протоколы хранятся в соответствии с ВД Банка, регулирующие вопросы делопроизводства.

172.Доступ работников или центра регистрации к закрытым ключам владельцев регистрационных свидетельств технически исключен использованием только защищенных носителей ключевой информации.

173.Целостность и принадлежность открытых ключей УЦ и его владельцев на этапе от их генерации до выпуска регистрационных свидетельств защищаются механизмом ЭЦП. Открытые ключи передаются от владельцев в УЦ только в форме электронных документов формата PKCS#10.

174.Открытые ключи УЦ передаются доверяющим сторонам в форме регистрационных свидетельств.

175.Владельцы регистрационных свидетельств могут запросить открытые ключи УЦ отдельно или как часть цепочки к собственному регистрационному свидетельству.

176.Открытые ключи УЦ (в составе регистрационных свидетельств) также доступны для загрузки с корпоративного интернет ресурса Банка.

177.УЦ выдает ключи, предназначенные для использования в соответствии с международным стандартом ГОСТ 34.310-2004 (ЭЦП):

Длина закрытого ключа – 256 двоичных разрядов.

Длина открытого ключа – 512 двоичных разрядов.

178.Закрытые ключи ЭЦП создаются УЦ в облачной ЭЦП.

179.Закрытые ключи облачной ЭЦП генерируются строго внутри HSM модуля. Закрытый ключ ЭЦП не извлекается из HSM в открытом виде. Требования к HSM модулям ЭЦП:

1) соответствует не ниже 3 (третьего) уровня безопасности в соответствии с требованиями, установленными СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования";

2) спроектирован с физической защитой периметра (защита от вскрытия корпуса), использующей датчики для определения факта вскрытия корпуса и последующего удаления ключевой информации, необходимой для HSM;

3) соответствует нормам эффективности защиты и методикам оценки защищенности информации и технических средств согласно требованиям действующего законодательства РК.

Все действия с носителями ключевой информации должны осуществляться строго в соответствии с инструкциями по их эксплуатации и требованиями безопасности.

§2. Защита закрытых ключей и инженерные контроли криптографических модулей

180.В центре сертификации закрытые ключи владельцев генерируются непосредственно на защищенном носителе ключевой информации, исключающем возможность его разглашения, изменения или несанкционированного использования.

181.Для выполнения операций с ключами УЦ, активированными внутри HSM, требуется участие не менее 2 (двоих) уполномоченных работников УЦ.

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

183.Генерация закрытых ключей УЦ производится центром сертификации непосредственно в том аппаратном криптографическом модуле (HSM), в котором эти ключи будут впервые использованы. Дополнительной активации вновь сгенерированных закрытых ключей не требуется.

184.Закрытые ключи УЦ после создания не подлежат депонированию. Вместе с тем, в целях обеспечения возможности восстановления функционирования ИС после чрезвычайного происшествия или иного сбоя в работе центр сертификации непосредственно после генерации каждого нового закрытого ключа создает и хранит резервную копию всех используемых в текущий момент закрытых х ключей.

185.В ходе создания резервной копии закрытые ключи зашифровываются и выгружаются Системным администратором УЦ из аппаратного криптографического модуля (HSM) в зашифрованном виде, в ходе восстановления – в обратном порядке, резервная копия загружается в HSM в зашифрованном виде, и закрытые ключи расшифровываются внутри устройства.

186.При выгрузке резервной копии закрытых ключей УЦ из аппаратного криптографического модуля (HSM) создается секрет (данные активации), который делится на n частей. Для активации ключей после их восстановления из резервной копии достаточно задействования m частей секрета при участии их хранителей. Текущее значение параметров m из n зафиксировано в паспорте HSM (на момент издания настоящих Правил n = 3 и m = 2)

187.Должностной состав хранителей частей секрета и резервных копий закрытых ключей УЦ фиксируется в протоколе генерации ключей УЦ.

188.В целях обеспечения непрерывности функционирования центра сертификации закрытые ключи в аппаратных криптографических модулях (HSM) после их генерации или восстановления из резервной копии остаются активированными до момента уничтожения (удаления).

189.Закрытые ключи УЦ, утратившие актуальность вследствие замены или истечения срока действия, уничтожаются Системным администратором УЦ штатными функциями аппаратных криптографических модулей (HSM) в соответствии с эксплуатационно-технической документацией сертифицированных средств криптографической защиты информации.

190.На этапе хранения резервная копия закрытых ключей УЦ защищена от разглашения, искажения и подмены криптографическими и организационными мерами.

191.Шифрование резервной копии закрытых ключей УЦ при их (за-)выгрузке (в) из аппаратного(-ый) криптографического (- ий) модуля(-ь) (HSM) осуществляется Системным администратором УЦ с созданием (использованием) данных активации в форме секрета, разделенного на части, каждая из которых закрепляется за отдельным ответственным лицом (хранителем части секрета), записывается на защищенный носитель информации и защищается персональным паролем.

192.Резервные копии закрытых ключей УЦ, утратившие актуальность вследствие замены или истечения срока действия, не подлежат архивному хранению и уничтожаются Системным администратором УЦ в соответствии с ВД Банка, регламентирующие процессы уничтожения электронной информации и неисправных электронных носителей.

193.Аппаратные криптографические модули (HSM), в которых когда-либо находились закрытые ключи продуктивной среды центра сертификации, выведенные из эксплуатации вследствие истечения срока эксплуатации или не поддающиеся ремонту после поломки, за исключением тестовых HSM, не подлежат выбытию из Банка или повторному использованию в любом ином качестве, включая разукомплектование на отдельные узлы и детали. После списания с баланса вышеуказанные HSM подлежат уничтожению в соответствии с ВД, регламентирующие процессы уничтожения электронной информации и неисправных электронных носителей.

§3. Иные аспекты управления ключами

194.Период использования любой пары ключей, открытый ключ из которой заверен регистрационным свидетельством, выпущенным УЦ, совпадает со сроком действия регистрационного свидетельства, за тем исключением, что в целях расшифрования информации или проверки ЭЦП соответствующие ключи могут использоваться и после истечения срока действия регистрационного свидетельства.

195.Срок действия регистрационного свидетельства УЦ составляет не менее 20 (двадцати) лет и исчисляется с даты и времени его выпуска.

196.Срок действия регистрационных свидетельств владельцев, поступившие через центр регистрации, составляют 1 (один) год и устанавливается нормативно-технической документацией, заинтересованной ИС Банка, в соответствии с параграфом 3 главы 3 Правил.

197.Для непрерывной работы в ИС, которые требуют наличия регистрационных свидетельств, выпущенных УЦ, владельцы в соответствии с Правилами наделены правом запрашивать выпуск нового регистрационного свидетельства для замены регистрационного свидетельства с истекающим сроком действия.

§4. Данные активации закрытого ключа

198.Для использования закрытого ключа владельцу УЦ необходимо создать и применять данные активации в форме пароля.

199.При установке пароля участник ИОК (за исключением владельцев регистрационных свидетельств) обязан произвести его смену (замену) сразу после первого подключения, при этом пароль:

1) не должен быть короче 8 (восьми) символов;
2) должен содержать минимум 1 (одну) букву в нижнем регистре (строчную);
3) должен содержать минимум 1 (одну) букву в верхнем регистре, 1 (одну) цифру или 1 (один) спецсимвол;

4) не должен содержать повторяющихся символов.

200.При установке пароля в центре регистрации владельцем регистрационного свидетельства вводится пароль, к которому установлены следующие требования:

1) не должен быть короче 4 (четырех) символов;

2) должен содержать только цифровые значения.

201.Запрещается записывать пароль доступа к ключу. Пароль должен быть известен только владельцу ключа. Запрещается использование функции автоматического сохранения пароля в используемых средствах безопасности.

202.Пароли для активации закрытого ключа владельца регистрационного свидетельства используются в соответствии с требованиями Правил идентификации и аутентификации пользователей в информационных системах.

203.Каждый хранитель (участник ИОК) части секрета, которая предназначена для активации закрытых ключей УЦ, хранит свой пароль в тайне и несет ответственность за нарушение данного требования, предусмотренную трудовым договором и должностной инструкцией.

204.Аппаратные токены, содержащие данные активации закрытых ключей УЦ, в случае утраты актуальности данных активации перезаписываются (обнуляются) и хранятся в порядке, предусмотренном для хранения резервных копий паролей, до момента повторного использования в тех же целях или до списания с обязательным последующим уничтожением. Выбытию из Банка, разукомплектованию или повторному использованию в иных целях защищенные носители, когда-либо использовавшиеся для хранения частей секрета, не подлежат.

§5. Контроль безопасности вычислительных ресурсов

205.Серверы для подписи регистрационных свидетельств, СОРС, ответов (квитанций) службы OCSP защищаются от несанкционированного доступа.

206.Операционные системы серверов поддерживаются на высоком уровне защиты путем применения рекомендованных пакетов защиты и обновлений, в том числе антивирусных в соответствии с ВД, регламентирующие процедуру обеспечения ИБ ИС.

207.Доступ к администрированию основных серверов разрешен только работникам, связанным с обслуживанием центра сертификации, остальные пользователи программных приложений УЦ не имеют доступа к системным или технологическим учетным записям.

208.Сегменты сети, используемые для обслуживания участников ИОК, логически отделены от остальной сети Банка. Это выделение исключает любой сетевой доступ пользователей к данным УЦ кроме доступа через определенные прикладные программные процессы. Прямой доступ к базам данных центра сертификации ограничен минимально необходимой группой Администраторов УЦ и Системных администраторов УЦ.

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

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

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

212.Функции УЦ выполняются в центре сертификации, защищенной от несанкционированного доступа в соответствии с ВД Банка, регламентирующим порядок защиты от несанкционированного доступа.

213.Схема взаимодействия модулей (компонент) УЦ с пояснительной запиской приведена в приложении 1 к Правилам.

§6. Контроль управления развитием и безопасностью сети

214.Все прикладное программное обеспечение, которое использует в своей деятельности УЦ, является лицензионным, исключительные права на него Банку не принадлежат.

215.Обязательства по обеспечению надлежащего функционирования прикладного программного обеспечения, которое использует в своей деятельности УЦ, выполняет поставщик по договору (сервисная организация).

216.В целях апробации любых изменений в центре сертификации имеет и поддерживает ее тестовый контур, обеспеченный необходимым минимумом вычислительной техники, средств криптографической защиты информации и лицензий на использование программного обеспечения.

217.Регистрационные свидетельства, СОРС, ответы квитанции (ответы службы) OCSP, контрольные протоколы центра сертификации, содержащие информацию о выпуске и изменении статуса регистрационных свидетельств, содержат информацию о дате и времени событий.

218.Информация о дате и времени событий, содержащаяся в регистрационных свидетельствах, СОРС, квитанциях (ответах службы) OCSP, заверяется ЭЦП УЦ.

Глава 8. Профили регистрационных свидетельств, СОРС и OCSP

§1. Профили регистрационных свидетельств

219.Регистрационные свидетельства, выпускаемые УЦ, соответствуют рекомендациям RFC 3280 с маркировкой по версии 3 (v.3).

220.Основные поля, содержащиеся в регистрационных свидетельствах, вместе с требованиями к их содержанию приведены в нижеуказанной таблице:

Название	Требования к содержанию
Version	V3
serialNumber	уникальный серийный номер регистрационного свидетельства
signatureAlgorithm	объектный идентификатор криптографического алгоритма, для которого предназначен ключ, указанный в поле subjectPublicKeyInfo
Issuer	C=KZ O=Jusan Bank JSC CN=Certification Authority
Validity	YYYYMMDDHHMMSSZ GMT (действителен с) YYYYMMDDHHMMSSZ GMT (действителен по)
Subject	C=KZ O= Jusan Bank JSC OU=Логическая или структурная единица Банка, например, информационная система или подсистема Банка, блок, департамент или иное подразделение Банка CN= код владельца (ФИО) UID= код владельца (ИИН)
subjectPublicKeyInfo	открытый ключ
issuerSignatureAlgorithm	объектный идентификатор криптографического алгоритма, которым подписано регистрационное свидетельство
signatureValue	электронная цифровая подпись

221.Имена, которые указываются в регистрационных свидетельствах, выпускаемых УЦ, соответствуют требованиям Правил, в соответствии с форматом имен ITU-T X.520.

222.Основные расширения, используемые в регистрационном свидетельстве, вместе с требованиями к их синтаксису приведены в нижеследующей таблице:

Название	Критичность	Формат
1	2	3
authorityKeyIdentifier	FALSE	согласно OID 2.5.29.35
subjectKeyIdentifier	FALSE	согласно OID 2.5.29.14
keyUsage	TRUE	согласно OID 2.5.29.15
CertificatePolicies	FALSE	согласно OID 2.5.29.32
basicConstraint	TRUE	согласно OID 2.5.29.19
1	2	3
extendedKeyUsage	FALSE	согласно OID 2.5.29.37
cRLDiistributionPoints	FALSE	согласно OID 2.5.29.31
authorityInformationAccess	FALSE	согласно OID 1.3.6.1.5.5.7.1.1 (RFC 2459)

223.Криптографический алгоритм, применяемый УЦ для подписи регистрационных свидетельств, приведен в нижеуказанной таблице:

Название	Формат
ГОСТ 34.310-2004	{iso(1) member-body(2) kz(398) certification-authorities(3) basic-cryptography(10) algorithms(1) digital-signature(1) GOST-34.310-2004(1)}

224.Схемы использования ЭЦП владельцев и получения регистрационного свидетельства ЭЦП владельцами с исходными данными (основными требованиями) к алгоритмам криптографических преобразований, применяемых в процессе формирования и использования регистрационного свидетельства ЭЦП, приведены в приложении 2 к Правилам.

225.Объектные идентификаторы политики регистрационных свидетельств, соответствующие информационным системам, в которых применяются регистрационные свидетельства, выпущенные УЦ, устанавливаются в соответствии с Правилами. Расширение регистрационных свидетельств «certificatePolicies» заполняется в соответствии с настоящей главой Правил.

§2. Профили списка отозванных регистрационных свидетельств

226.СОРС, выпускаемые УЦ, соответствуют рекомендациям RFC 3280 с маркировкой по версии 2 (v.2).

227.Основные поля и расширения, содержащиеся в СОРС, вместе с требованиями к их содержанию приведены в нижеуказанной таблице:

Название	Требования к содержанию
Version (optional)	V2
Issuer	C=KZ O=Jusan Bank JSC CN=Certification Authority
thisUpdate	YYYYMMDDHHMMSSZ GMT (действителен с)
[nextUpdate (optional)	YYYYMMDDHHMMSSZ GMT (следующее обновление)
signatureAlgorithm	объектный идентификатор алгоритма, которым подписан список отозванных регистрационных свидетельств
revokedCertificates	Последовательность пар следующего вида: 1. certificateSerialNumber (серийный номер регистрационного свидетельства); 2. Time (время обработки заявления на отзыв регистрационного свидетельства).
cRLNumber	номер СОРС
authorityKeyIdentifier	идентификатор ключа удостоверяющего центра
signatureValue	электронная цифровая подпись

228.Расширения, используемые в записях СОРС, которые выпускает УЦ, приведены в нижеуказанной таблице:

Название	Критичность
reasonCode	FALSE
certificateIssuer	FALSE

§3. Профиль сервиса OCSP

229.Протокол OCSP необходим доверяющим сторонам для определения статуса указанного регистрационного свидетельства в текущий момент времени.

230.Сервис OCSP для получения информации о статусе регистрационных свидетельств, выпущенных УЦ, предоставляется центром сертификации в формате версии 1 (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).

Глава 9. Проверка деятельности

231.Аккредитация УЦ осуществляется на бесплатной основе сроком на 3 (три) года в соответствии с законодательством РК «Об электронном документе и электронной цифровой подписи».

232.Деятельность подразделений, участвующих в обеспечении работы УЦ (Администратора УЦ, Системного администратора УЦ, Офицера безопасности УЦ, Начальника УЦ, Дежурного УЦ), на плановой основе подвергается внутреннему аудиту в соответствии с ВД Банка, регламентирующим порядок проведения аудита.

Глава 10. Прочие вопросы

§1. Тарифы

233.Центр сертификации предоставляет пользователям обслуживаемых информационных систем следующие услуги, которые не тарифицируются и не оплачиваются:

1) выпуск регистрационного свидетельства по заявлениям физических лиц;

2) отзыв регистрационного свидетельства;

3) размещение регистрационных свидетельств и СОРС в хранилище;

4) предоставление информации о статусе регистрационных свидетельств в режиме онлайн по протоколу OCSP;

5) привязка данных к реальному времени в режиме онлайн по протоколу TSP (Time stamp protocol - сервис «метки времени»).

§2. Защита персональных данных участников

234.Любой владелец регистрационного свидетельства признает, что, подавая заявление на выпуск регистрационного свидетельства в УЦ, он дает согласие на размещение содержащейся в нем информации о себе в публичном доступе.

235.Заявление на выпуск регистрационного свидетельства является письменным документом, означающим согласие субъекта на сбор и обработку его персональных данных в соответствии с законодательством РК по вопросам персональных данных владельцев регистрационных свидетельств и их защиты.

236.УЦ обеспечивает защиту сведений о владельцах регистрационных свидетельств и раскрывает их в случаях, предусмотренных законодательством РК.

237.Сведения о владельцах регистрационных свидетельств, являющиеся конфиденциальными в соответствии с соглашением сторон, не включаются в общедоступный регистр регистрационных свидетельств.

§3. Права интеллектуальной собственности

238.Владельцы регистрационных свидетельств сохраняют все свои права на имена и торговые марки, содержащиеся в регистрационных свидетельствах.

239.УЦ не запрещает владельцам и пользователям регистрационных свидетельств (владельцем и доверяющим сторонам) копирование и распространение регистрационных свидетельств на неисключительной бесплатной основе, при соблюдении условий полноты и целостности данных.

240.Закрытый ключ, который соответствует регистрационному свидетельству, выпущенному УЦ, является собственностью владельца этого регистрационного свидетельства. Соответствующий ему открытый ключ и регистрационное свидетельство являются собственностью Банка.

§4. Гарантии и заверения

241.Центр сертификации обеспечивает:

1) соответствие данных, содержащихся в выпущенных им регистрационных свидетельствах, тем сведениям, которые предоставил центр регистрации в составе запроса на выпуск регистрационного свидетельства, и отсутствие в данных регистрационных свидетельствах случайных или умышленных искажений этих сведений по умыслу или в результате ошибочных действий работников УЦ;

2) соответствие оказываемых услуг (выпуск, отзыв регистрационных свидетельств, выпуск CORC, онлайн-сервисы OCSP и TSP), требованиям: действующего законодательства РК по вопросам электронного документа и электронной цифровой подписи, Политики и Правил;

3) публикацию требований Политики и Правил на корпоративном интернет ресурсе Банка.

242.Центр регистрации обеспечивает:

1) соответствие данных в направляемых в центр сертификации запросах на выпуск регистрационного свидетельства, сведениям из тех документов, которые предоставил заявитель в ходе процедур идентификации, и отсутствие в данных запросах умышленных или случайных искажений, внесенных по умыслу или допущенных в результате ошибочных действий бизнес-владельцев ИС;

2) соответствие выполняемых центром регистрации процедур (регистрация и обработка заявлений заявителей на выпуск и отзыв регистрационных свидетельств, процедуры идентификации заявителей, выдача регистрационных свидетельств владельцу) и требованиям действующего законодательства РК по вопросам электронного документа и электронной цифровой подписи, Политики и Правил.

243. Каждый владелец регистрационного свидетельства обеспечивает:

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

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

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

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

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

245.Центр сертификации не несет перед владельцами и пользователями регистрационных свидетельств (владелец и доверяющими сторонами) дополнительной ответственности, вытекающей из договоров оказания банковских услуг, включая ответственность за товарную пригодность и соответствие, кроме той ответственности, которая установлена законодательством РК по вопросам электронного документа и ЭЦП и задекларирована Политикой.

§5. Уведомления и связь с участниками

246.Участники ИОК: работники УЦ, владельцы и пользователи регистрационных свидетельств (владельцы и доверяющие стороны) - для связи друг с другом используют любые целесообразные каналы, соответствующие предмету взаимодействия, степени важности и срочности коммуникации (корпоративный интернет ресурс, электронная почта (e-mail), почтовая связь, телефонная связь, мобильное приложение, интернет-банкинг, телебанкинг, телефон, и иные интернет-ресурсы), если иное не определено соглашением между сторонами.

§6. Разрешение споров

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

248.Для разрешения споров, предметом которых являются разногласия по существу настоящих Правил, применяется законодательство РК.

249.В случае наступления обстоятельств непреодолимой силы (форс-мажор) участники ИОК: работники УЦ, владельцы и пользователи регистрационных свидетельств (владельцы и доверяющие стороны) - руководствуются соответствующими положениями действующих между ними договоров (при наличии).

Глава 11. Ответственность

250.Ответственность участников ИОК, обслуживаемой УЦ, установлена законодательством РК.

251.Ответственность работников, связанных с обслуживанием центра сертификации и центра регистрации (Администратора УЦ, Системного администратора УЦ, Офицера безопасности УЦ, Начальника УЦ, Дежурного УЦ) установлена трудовым договором и должностными инструкциями.

252.В части, не противоречащей действующему законодательству РК, центр регистрации несет ответственность за:

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

2) непреднамеренное или умышленное сокрытие существенных фактов, подлежащих отражению в заявлении на выпуск или отзыв регистрационного свидетельства.

253.В части, не противоречащей действующему законодательству РК, владельцы регистрационных свидетельств несут ответственность за:

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

2) непреднамеренное или умышленное сокрытие существенных фактов, подлежащих отражению в заявлении на выпуск или отзыв регистрационного свидетельства;

3) использование в составе своего выделенного имени названий, нарушающих права интеллектуальной собственности третьих лиц.

254.В части, не противоречащей действующему законодательству РК, пользователи регистрационных свидетельств (доверяющие стороны) несут ответственность за:

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

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

255.Ответственность за надлежащее исполнение Правил возлагается на работников и руководителей УЦ, указанных в пункте 251 Правил.

256.Ответственность за ненадлежащее исполнение Правил возлагается на работников и руководителей УЦ, указанных в пункте 251 Правил.

257.Руководитель подразделения цифрового развития несет ответственность за организацию и поддержание эффективного внутреннего контроля в соответствии с положениями ВД Банка, регламентирующих политику внутреннего контроля и процедуру осуществления внутреннего контроля в Банке.

258.Руководители и работники УЦ, указанных в пункте 251 Правил, участвующие в деятельности УЦ несут ответственность за организацию и осуществление внутреннего контроля в соответствии с положениями ВД Банка, регламентирующих политику внутреннего контроля и процедуру осуществления внутреннего контроля в Банке.

259.Руководители и работники УЦ, указанные в пункте 251 Правил, участвующие в деятельности УЦ, обязаны строго придерживаться принципа недопущения конфликта интересов при исполнении своих функциональных обязанностей и несут ответственность за соблюдение положений ВД Банка, регламентирующих политику управления конфликтами интересов в Банке. В случае возникновения конфликта интересов руководители и работники УЦ, оповещают об этом непосредственного руководителя и подразделение по управлению комплаенс-риском.

Глава 12. Конфиденциальность

260.За исключением информации, доступной в хранилище УЦ, согласно главе 3 Правил, иная информация о деятельности УЦ классифицируется в качестве конфиденциальной в соответствии с ВД Банка по вопросам отнесения тех или иных сведений к банковской/коммерческой тайне. Данным документом регламентируется ответственность участников ИОК и порядок обращения их в УЦ с указанной информацией.

261.Заявление на выпуск регистрационного свидетельства подтверждает согласие заявителя на сбор и обработку его персональных данных в соответствии с законодательством РК по вопросам персональных данных и их защиты, в том числе дает УЦ разрешение на публикацию регистрационных свидетельств заявителя и информации об их статусе в хранилище.

Глава 13. Заключительные положения

262.Правила актуализируются УЦ, расположенным по адресу: 050059, г. Алматы, Медеуский р-н, пр. Нұрсұлтан Назарбаев, д. 242.

263.Контактное лицо по вопросам актуализации документа – Руководитель УЦ, 050059, г. Алматы, Медеуский р-н, пр. Нұрсұлтан Назарбаев, д. 242, +7(727) 331 26 04 (вн. ____), _____@jusan.kz.

264.Правила применяются в соответствии с Политикой.

265.Правила публикуются по истечении 5 (пяти) рабочих дней со дня утверждения Правлением, если решением Правления не установлен иной срок.

266.Правила в том числе с учетом изменений и дополнений к ним вступают в силу со дня опубликования на корпоративном интернет ресурсе Банка. Положения, не урегулированные Правилами, регулируются законодательством РК и ВД Банка.

267.В случае изменения законодательства РК и возникновения противоречий отдельных положений Правил законодательству РК, такие положения Правил утрачивают силу, и работники Банка руководствуются в своей деятельности законодательством РК до соответствующей актуализации Правил.

268.В случае внесения изменений и дополнений в Правила, Правила утверждаются Правлением Банка в новой редакции.

269.Публикация новой утвержденной редакции Правил является официальным уведомлением о вступлении ее в силу для пользователей всех регистрационных свидетельств, выпущенных УЦ, включая их владельцев.

270.С даты публикации новой редакции Правил, если иное не предусмотрено переходными положениями утверждающего решения, изменения и дополнения становятся обязательными для применения пользователями всех регистрационных свидетельств, выпущенных УЦ, включая их владельцев.

271.Правила, с учетом публикуемых изменений и дополнений к ним, сохраняет силу до момента опубликования новой редакции Правил на корпоративном интернет ресурсе Банка.

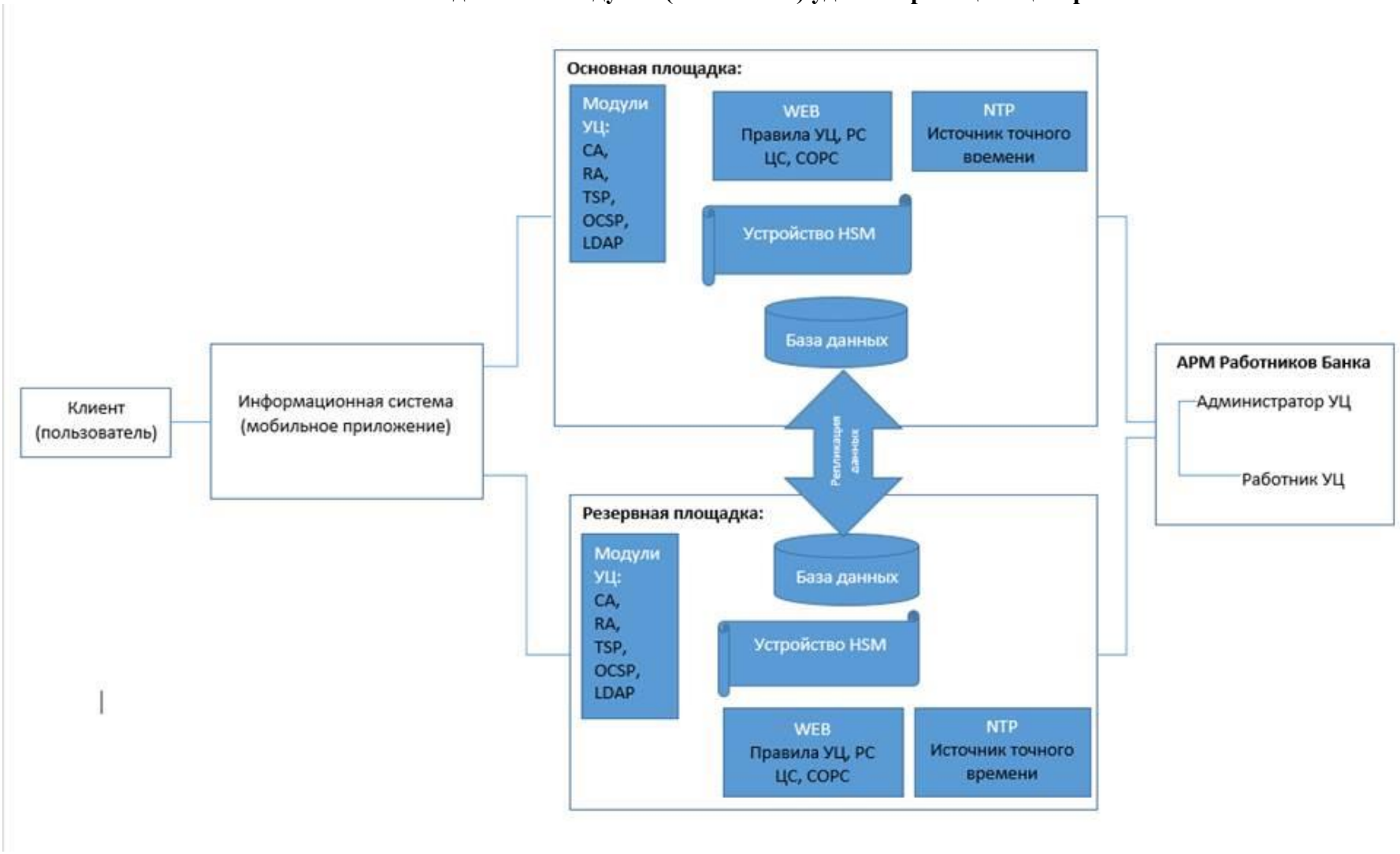
272.В случае отмены Правил участники ИС, которые используют регистрационные свидетельства, выпущенные УЦ, остаются связанными требованиями Политики до момента истечения периода действия регистрационных свидетельств.

273.В случае если часть положений Правил будет признана неприменимой судом или уполномоченным государственным органом, остальная их часть сохраняет силу.

274.В случае наступления обстоятельств непреодолимой силы (форс-мажор) участники ИОК: Удостоверяющий центр, владельцы и пользователи регистрационных свидетельств (владельцы и доверяющие стороны) - руководствуются соответствующими положениями действующих между ними договоров (при наличии).

Приложение 1
к Правилам деятельности удостоверяющего центра

Схема взаимодействия модулей (компонент) удостоверяющего центра



ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к Схеме взаимодействия модулей (компонент) Удостоверяющего центра
Взаимодействие компонентов (основной и резервный центр)

Взаимодействие модулей центра сертификации с хранилищем УЦ для публикации и поиска регистрационных свидетельств, СОРС осуществляется по протоколу LDAP.

Все модули УЦ используют единое время, получаемое от источника точного времени по протоколу NTP.

Безопасность взаимодействия модулей УЦ обеспечивается использованием сертифицированного средства криптографической защиты информации «ТУМАР-CSP», соответствующего 3 (третьему) уровню безопасности согласно СТ РК 1073-2007.

Для хранения и обеспечения безопасности закрытых ключей УЦ используются защищенные программно-аппаратные комплексы HSM, соответствующие 2 (второму) уровню безопасности согласно СТ РК 1073-2007.

В системе задействованы межсетевые экраны, контролирующие и фильтрующие весь поступающий сетевой трафик.

Взаимодействие между рабочим и резервным серверами центров обработки данных

Хранение и управление данными обеспечивается СУБД PostgreSQL

Между основным и резервным центрами средствами СУБД в режиме реального времени выполняется репликация данных, что повышает отказоустойчивость системы.

Защита реплицируемых данных обеспечивается шифрованием с применением протокола TLS.

Взаимодействие пользователей с Удостоверяющим центром

Владелец регистрационного свидетельства и доверяющая сторона напрямую с сервисами УЦ не взаимодействуют.

Взаимодействие осуществляется через целевые (обслуживаемые) центры регистрации, которые имеют возможность взаимодействия с LDAP-хранилищем и модулями центра сертификации с использованием протоколов LDAP и HTTP(S).

Взаимодействие работников УЦ с модулями Удостоверяющего центра

Взаимодействие работников УЦ, указанных в объектном идентификаторе политики с модулями центра сертификации осуществляется посредством специализированного программного обеспечения с использованием протоколов LDAP и HTTP(S).

Доступ с рабочего места вышеуказанного работника УЦ к модулям центра сертификации возможен только при наличии действующего регистрационного свидетельства с определенными свойствами.

Дополнительно, безопасность обеспечивается ограничением сетевого доступа только определенным набором IP адресов.

Приложение 2
к Правилам деятельности удостоверяющего центра

Схемы электронной цифровой подписи с данными о применяемых алгоритмах криптографических преобразований и другими исходными данными (основными требованиями) по реализации процесса формирования электронной цифровой подписи и требованиями к отдельным параметрам и удостоверяющему центру