Приложение к
Протоколу Правления
АО «Банк ЦентрКредит»
№1003/2 от 03.10. 2024 г.

РЕГЛАМЕНТ ДЕЯТЕЛЬНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА АО «БАНК ЦЕНТРКРЕДИТ»

Версия 2.1.1

Алматы 2024

Содержание

Глава 1. ВВЕДЕНИЕ

Раздел 1.1. Общие положения

1. Настоящий Регламент деятельности удостоверяющего центра АО «Банк ЦентрКредит» (далее – Регламент) разработан 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), и определяет порядок его функционирования.

2. Регламент разработан 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. Удостоверяющий центр АО «Банк ЦентрКредит» создан для оказания услуг по выдаче регистрационных свидетельств физическим лицам – клиентам АО «Банк ЦентрКредит» на основании действующего законодательства Республики Казахстан:

1) Закон Республики Казахстан «Об информатизации»;

2) Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи»;

3) Закон Республики Казахстан «О персональных данных и их защите»;

4) правовой акт по вопросам создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющих центрах[1] (далее – Правила облачной ЭЦП);

5) правовой акт по вопросам проверки подлинности электронной цифровой подписи[2] (далее – Правила проверки ЭЦП);

6) правовой акт по вопросам выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющими центрами[3] (далее – Правила выпуска и отзыва регистрационных свидетельств);

7) СТ РК 1073–2007. Средства криптографической защиты информации. Общие технические требования (далее – Стандарт).

4. Регламент определяет меры, реализуемые Удостоверяющим центром при обеспечении набора сервисов, который определен Политикой применения регистрационных свидетельств удостоверяющего центра АО «Банк ЦентрКредит» (далее – Политика регистрационных свидетельств) и включает в себя, но не ограничивается выпуском, управлением и отзывом регистрационных свидетельств.

5. 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.

6. Регламент, в отличие от Политики регистрационных свидетельств, определяет порядок и процедуры, в соответствии с которыми:

1) выполняются функции (работают сервисы) Удостоверяющего центра;

2) обеспечивается безопасность и управление ядром инфраструктуры открытых ключей.

На дату утверждения Регламента действуют:

[1] Правила создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре, в редакции с изменениями, внесенными приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 17 марта 2023 № 95/НҚ;

[2] Правила проверки подлинности электронной цифровой подписи, в редакции с изменениями, внесенными приказом Министра информации и коммуникаций РК от 30 декабря 2016 года № 316;

[3] 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, в редакции с изменениями, внесенными приказом и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 30 марта 2023 года № 115/НҚ.

7. С момента подачи участником информационной системы, использующей сервисы Удостоверяющего центра, заявки на выдачу регистрационного свидетельства, для участника становятся обязательными к выполнению применимые к нему требования той Политики регистрационных свидетельств, ссылка на которую содержится в заявке, и Регламента.

8. Регламент также определяет процедуры проверки, связанные с выпуском и дальнейшим обслуживанием тех видов регистрационных свидетельств, которые выпускает Удостоверяющий центр, в соответствии с Политикой регистрационных свидетельств.

Раздел 1.2. Наименование и атрибуты документа

9. Полное наименование документа – Регламент деятельности удостоверяющего центра АО «Банк ЦентрКредит».

10. Объектный идентификатор – 1.2.398.3.24.1.2.1.

11. Версия документа – 2.1.1.

12. Адрес сервера для публикации Регламента – https://www.bcc.kz/product/pki/?tab=DPP.

Раздел 1.3. Участники инфраструктуры открытых ключей

1.3.1. Центр сертификации

13. Центр сертификации – в контексте Регламента данным термином обозначается программно-аппаратный комплекс для выпуска, обслуживания и отзыва регистрационных свидетельств ключей, аккредитованный в соответствии с законодательством и действующий в соответствии с Регламентом.

14. Центр сертификации осуществляет следующие функции инфраструктуры открытых ключей:

1) обработка запросов на выпуск и отзыв регистрационных свидетельств;

2) публикация списков отозванных регистрационных свидетельств;

3) обработка запросов к службе протокола проверки статуса регистрационного свидетельства в режиме онлайн;

4) обработка запросов к службе протокола метки времени.

15. Маркировка Центра сертификации в регистрационных свидетельствах:

C = KZ,

O = Bank CenterCredit JSC,

CN = Certification Authority

1.3.2. Центр регистрации

16. Центр регистрации – в контексте Регламента данным термином обозначается информационная система АО «Банк ЦентрКредит», ответственная за прием и проверку документов на выпуск и/или отзыв регистрационных свидетельств, а также идентификацию и аутентификацию заявителей.

1.3.3. Владелец регистрационного свидетельства

17. Понятие «владелец регистрационного свидетельства» определено Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи» как «физическое или юридическое лицо, на имя которого выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве».

18. Без ограничения общности определения, установленного вышеуказанным Законом, в контексте Регламента термином «владелец регистрационного свидетельства» обозначаются любое физическое лицо, использующее информационные системы АО «Банк ЦентрКредит», а также любой работник Удостоверяющего центра, владеющий технологическим регистрационным свидетельством, если регистрационное свидетельство для них выпустил Удостоверяющий центр.

1.3.4. Доверяющая сторона

19. Доверяющая сторона – в контексте Регламента данным термином обозначается владелец регистрационного свидетельства или любое другое физическое лицо, использующее в информационных системах АО «Банк ЦентрКредит» 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

20. Назначением регистрационного свидетельства, выданного Удостоверяющим центром, является подтверждение соответствия электронной цифровой подписи требованиям, установленным законодательством, что определяет цель использования пары ключей электронной цифровой подписи, открытый из которых содержится в регистрационном свидетельстве.

21. В соответствии с разделом 1.4 Политики регистрационных свидетельств, в регистрационных свидетельствах, выпускаемых Удостоверяющим центром, в расширении “cerificatePolicies” присутствуют объектные идентификаторы политики, определяющие дополнительно область их применения.

22. Полный перечень объектных идентификаторов политики, указываемых Удостоверяющим центром в выпускаемых клиентских регистрационных свидетельствах, приведен на официальном информационном ресурсе АО «Банк ЦентрКредит» в сети Интернет по адресу https://www.bcc.kz/product/pki/?tab=OIPS.

Раздел 1.5. Управление документом

23. Регламент актуализируется Дирекцией криптографической защиты информации (Удостоверяющим центром), расположенным по адресу: A05G1D2, г. Алматы, ул. Панфилова, д. 98, блок Б.

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

25. Изменения и дополнения в Регламент готовятся Удостоверяющим центром либо в форме новой редакции документа, либо в форме перечня изменений и дополнений к текущей его редакции.

26. Перед утверждением изменения и дополнения в Регламент проходят согласование с заинтересованными подразделениями и должностными лицами АО «Банк ЦентрКредит» согласно внутренним процедурам, за исключением незначительных (изменение адресов и ссылок, контактной информации, исправления опечаток и др.).

27. Изменения и дополнения в Регламент утверждаются протокольным решением Правления АО «Банк ЦентрКредит», за исключением незначительных (изменение адресов и ссылок, контактной информации, исправления опечаток и др.).

28. Все изменения и дополнения в Регламент публикуются на официальном информационном ресурсе АО «Банк ЦентрКредит» в сети Интернет по адресу https://www.bcc.kz/product/pki/?tab=DPP.

29. Публикация новой утвержденной редакции Регламента в разделе «Действующие редакции» является официальным уведомлением о вступлении ее в силу для всех владельцев регистрационных свидетельств, выпущенных Удостоверяющим центром, и всех доверяющих сторон.

30. С даты официального уведомления о вступлении в силу новой редакции Регламента, если иное не предусмотрено переходными положениями утверждающего решения, изменения и дополнения становятся обязательными для применения всеми владельцами регистрационных свидетельств, выпущенных Удостоверяющим центром, и всеми доверяющими сторонами.

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

32. Существенные изменения и дополнения в Регламент Удостоверяющий центр предварительно публикует, в форме проекта, на официальном информационном ресурсе АО «Банк ЦентрКредит» в сети Интернет по адресу https://www.bcc.kz/product/pki/?tab=DPP, как правило не менее чем за 14 календарных дней до вступления в силу, если иное не предусмотрено опубликованными изменениями в законодательстве Республики Казахстан.

Раздел 1.6. Термины, определения и сокращения

33. Термины «удостоверяющий центр», «аккредитация удостоверяющего центра», «регистрационное свидетельство», «владелец регистрационного свидетельства», «электронный документ», «электронный документооборот», «электронная цифровая подпись», «открытый ключ электронной цифровой подписи», «закрытый ключ электронной цифровой подписи» применяются в Регламенте в соответствии со значениями, установленными Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи».

34. Значение и применение терминов «Центр сертификации», «Центр регистрации», «доверяющая сторона», а также особенности применения в документе термина «владелец регистрационного свидетельства» приведены в разделе 1.3. Регламента.

35. Другие специальные термины, применяемые в Регламенте, используются в следующем значении:

Термин	Определение
Аппаратный криптографический модуль (Hardware Security Module)	Аппаратный криптографический модуль, предназначенный для шифрования информации и управления открытыми и закрытыми ключами электронной цифровой подписи
Аутентификация	Процесс или сервис безопасности, реализующий этот процесс, который предназначен для проверки того, что лицо (предмет) является тем, кем себя именует (чем он поименован)
Банк	АО «Банк ЦентрКредит»
Биометрическая аутентификация	Комплекс мер, идентифицирующих личность на основании физиологических и неизменных биологических признаков
Блокчейн	Информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе данных на базе цепочки взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования
Данные активации	Любые данные, за исключением целых криптографических ключей, которые необходимы для выполнения криптографических преобразований и требуют защиты: персональные идентификационные номера (PIN), парольные фразы, компоненты разделенного криптографического ключа, биометрические параметры и др.
Заявитель	Физическое лицо, подавшее документы на выдачу или отзыв регистрационного свидетельства
Идентификация	Процесс (или результат процесса), который устанавливает идентичность физического или юридического лица (показывающий, что данное лицо является однозначно определенным 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)
Информационная система	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
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
Компрометация ключей электронной цифровой подписи	Утрата владельцем регистрационного свидетельства уверенности в том, что конкретные ключи электронной цифровой подписи обеспечивают безопасность защищаемой с их помощью информации

Термин	Определение
Многофакторная 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)
Носитель ключевой информации	Специализированный носитель, в котором для защиты хранящихся закрытых ключей электронной цифровой подписи используется средство криптографической защиты информации, имеющее сертификат соответствия требованиям Стандарта
Облачная ЭЦП	Сервис удостоверяющего центра, позволяющий создавать, использовать, хранить и удалять закрытые ключи электронной цифровой подписи в HSM удостоверяющего центра, где доступ к закрытому ключу осуществляется владельцем удалённо посредством не менее двух факторов аутентификации, одним из которых является биометрическая
Объект	Алгоритм, информационная система, а также другие элементы, используемые физическими и юридическими лицами для электронного документооборота
Объектный идентификатор	Уникальный набор цифр, который связан с объектом и однозначно идентифицирует его в мировом адресном пространстве объектов
Отозванное регистрационное свидетельство	Регистрационное свидетельство, аннулированное в порядке, который установлен Правилами выпуска и отзыва регистрационных свидетельств
Политика применения регистрационных свидетельств	Внутренний документ, утвержденный удостоверяющим центром, определяющий регламент и механизмы работы удостоверяющего центра в части управления регистрационными свидетельствами
Приложение ВСС	Мобильные приложения/цифровые платформы Банка, предоставляющие услуги дистанционного банковского обслуживания для физических лиц
Протокол метки времени	Криптографический протокол, позволяющий создавать доказательство факта существования электронного документа на определённый момент времени
Регламент деятельности удостоверяющего центра	Документ, который определяет порядок организации основной деятельности удостоверяющего центра, осуществляемой в соответствии с политикой применения регистрационных свидетельств, включая реализацию основных процессов удостоверяющего центра
Список отозванных регистрационных свидетельств	Часть регистра регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва (аннулирования)
Средство криптографической защиты информации	Средство, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами
Участники инфраструктуры открытых ключей	Совокупность физических и юридических лиц, которые выполняют любую из ролей в одной и той же инфраструктуре открытых ключей: роль владельца регистрационного свидетельства или доверяющей стороны, – а также удостоверяющего центра и центра(-ов) регистрации
Хэш	Преобразование массива входных данных произвольной длины в битовую строку фиксированной длины

36. В тексте Регламента используются следующие сокращения:

Аббревиатура	Определение
DN	Отличительное имя (Distinguished Name)
HSM	Аппаратный криптографический модуль (Hardware Security Module)
LDAP	Протокол облегченного доступа к каталогам (Lightweight Directory Access Protocol)
OCSP	Протокол проверки статуса регистрационного свидетельства в режиме онлайн (Online Certificate Status Protocol)
OID	Объектный идентификатор (Object Identifier)
TSP	Протокол метки времени (Time Stamp Protocol)
ИОК	Инфраструктура открытых ключей
ИС	Информационная система
НКИ	Носитель ключевой информации

Аббревиатура	Определение
СКЗИ	Средство(-а) криптографической защиты информации
СОРС	Список отозванных регистрационных свидетельств
УЦ	Удостоверяющий центр АО «Банк ЦентрКредит»
ЦР	Центр регистрации
ЭЦП	Электронная цифровая подпись

Глава 2. ОТВЕТСТВЕННОСТЬ ЗА ХРАНИЛИЩЕ И ПУБЛИКАЦИЮ ДАННЫХ В НЕМ

Раздел 2.1. Хранилище

37. УЦ предоставляет для скачивания и ознакомления следующие документы:

1) Политика регистрационных свидетельств https://www.bcc.kz/product/pki/?tab=DPP;
2) Регламент https://www.bcc.kz/product/pki/?tab=DPP;
3) СОРС https://uc.bcc.kz/cgi/crl.

38. Через приложение ВСС пользователям приложения, а также работникам ЦР обеспечивается доступность подачи запросов к следующим сервисам УЦ:

1) OCSP https://bcc-app.bank.corp.centercredit.kz:62301/
2) TSP https://bcc-app.bank.corp.centercredit.kz:62302/
3) Центр сертификации https://bcc-app.bank.corp.centercredit.kz:62305/
4) ЦР https://bcc-app.bank.corp.centercredit.kz:62310/

Раздел 2.2. Публикация **в хранилище информации о регистрационных свидетельствах**

39. Каждому участнику ИОК в хранилище публикуются выпущенные на его имя регистрационные свидетельства, а также СОРС.

Раздел 2.3. Периодичность актуализации данных в хранилище

40. Выданные регистрационные свидетельства и СОРС вносятся в хранилище и публикуются не позднее даты начала их действия.

41. Публикация СОРС производится по мере появления отозванных регистрационных свидетельств. При этом период обновления СОРС не превышает 7 календарных дней,

42. Сведения о статусе регистрационного свидетельства публикуются в соответствии с Регламентом.

Раздел 2.4. Контроль доступа к хранилищу

43. Доступ к хранилищу осуществляется по LDAP в соответствии с RFC 2251 (Lightweight Directory Access Protocol (v3) – Протокол облегченного доступа к каталогам (версия 3)). УЦ осуществляет защиту от несанкционированного доступа к хранилищу.

44. Сведения, публикуемые на странице УЦ официального информационного ресурса Банка в сети Интернет, предоставляются участникам ИС в режиме свободного доступа, с правами «только для чтения».

Глава 3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Раздел 3.1. Требования к именам

45. УЦ выдает регистрационные свидетельства, соответствующие рекомендациям X.509 ITU-T версии 3 и RFC 3280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile». Регистрационное свидетельство содержит в поле «Subject» DN в формате, рекомендуемом стандартом X.520 ITU-T. DN регистрационного свидетельства содержит персональные данные, позволяющие идентифицировать его владельца. DN определяет владельца регистрационного свидетельства и соответствующего закрытого ключа, а также позволяет определить область применения регистрационного свидетельства.

46. Каждому владельцу регистрационного свидетельства соответствует уникальное DN.

47. Однозначность идентификации достигается за счет использования индивидуальных идентификационных номеров (ИИН) из единого республиканского реестра, на основании используемых методов идентификации и аутентификации.

48. Анонимность и использование псевдонимов при формировании DN не допускается.

Раздел 3.2. Первоначальная проверка идентичности

3.2.1. Идентификация и аутентификация при выпуске регистрационного свидетельства для обслуживаемых физических лиц

49. При подаче заявки на выдачу регистрационного свидетельства обслуживаемое физическое лицо проходит процедуру многофакторной аутентификации, включая биометрическую аутентификацию, в соответствии с Правилами облачной ЭЦП.

3.2.2. Идентификация и аутентификация при выпуске технологического регистрационного свидетельства (для служебных пользователей УЦ)

50. Перед регистрацией заявки на выдачу регистрационного свидетельства идентификация и аутентификация заявителя проводится по документам, удостоверяющим его личность, содержащим его индивидуальный идентификационный номер, а также наделяющим его правом представлять Банк в вопросах работы с УЦ, в соответствиии с Правилами выпуска и отзыва регистрационных свидетельств.

Раздел 3.3. Идентификация и аутентификация при запросах на смену ключей электронной цифровой подписи

51. Процедуры идентификации и аутентификации при обработке заявки и смене ключей ЭЦП полностью аналогичны процедурам идентификации и аутентификации при обработке заявки н выпуске регистрационного свидетельства, изложенным в разделе 3.2.

Раздел 3.4. Идентификация и аутентификация при отзыве регистрационного свидетельства

3.4.1. Идентификация и аутентификация при отзыве регистрационного свидетельства для обслуживаемых лиц

52. Подача заявок на отзыв регистрационных свидетельств для обслуживаемых физических лиц осуществляется через дистанционный канал (приложение ВСС). В процессе отзыва регистрационного свидетельства заявитель должен:

1) пройти процедуру биометрической аутентификации;

2) ввести пароль от закрытого ключа ЭЦП, соответствующего регистрационному свидетельству, и указать причину отзыва.

3.4.2. Идентификация и аутентификация при отзыве технологического регистрационного свидетельства (для служебных пользователей УЦ)

53. Перед регистрацией заявки на отзыв регистрационного свидетельства идентификация и аутентификация заявителя проводится по документам, удостоверяющим его личность, содержащим его индивидуальный идентификационный номер, а также наделяющим его правом представлять Банк в вопросах работы с УЦ, в соответствиии с Правилами выпуска и отзыва регистрационных свидетельств.

Глава 4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА

Раздел 4.1. Заявки на выдачу регистрационного свидетельства

54. Заявку на выдачу регистрационного свидетельства имеют право подавать физические лица, имеющие индивидуальный идентификационный номер РК.

55. Подача заявок на выдачу регистрационных свидетельств для обслуживаемых физических лиц осуществляется через дистанционный канал (приложение ВСС). Заявка создается в электронном виде, ее форма приведена в приложении 1 к Регламенту.

56. Подача заявок на выдачу технологического регистрационного свидетельства для служебных пользователей УЦ осуществляется путем личной явки в УЦ, заполнения заявления на выдачу регистрационного свидетельства по форме Правил выпуска и отзыва регистрационных свидетельств и его заверения личной подписью заявителя.

57. В контексте Регламента заявка на выдачу регистрационного свидетельства означает или электронную заявку по форме приложения 1 к Регламенту, или заявление в виде документа на бумажном носителе по форме Правил выпуска и отзыва регистрационных свидетельств.

58. В процессе подачи заявки на выдачу регистрационного свидетельства заявитель должен:

1) дать согласие (надлежащим образом заверить утвержденную форму Банка) на сбор и обработку персональных данных;

2) ознакомиться с Политикой регистрационных свидетельств и Регламентом;

3) ознакомиться с текстом заявки на выдачу регистрационного свидетельства.

Раздел 4.2. Обработка заявок на выдачу регистрационного свидетельства

59. В процессе обработки заявок на выдачу регистрационного свидетельства проводится процедура идентификации и аутентификации заявителя, изложенная в разделе 3.2.

Обслуживаемые физические лица подвергаются многофакторной аутентификации, в соответствии с Правилами облачной ЭЦП, включая биометрическую аутентификацию, через дистанционный канал (приложение ВСС).

Служебные пользователи УЦ идентифицируются и аутентифицируются при личной явке в УЦ, в соответствии с Правилами выпуска и отзыва регистрационных свидетельств.

60. В выдаче регистрационного свидетельства отказывается в случаях, когда:

1) заявителем не представлена (либо представлена не полностью) необходимая информация;

2) заявителем представлена недостоверная информация;

3) заявитель не достиг шестнадцатилетнего возраста;

4) имеется вступившее в законную силу решение суда.

Раздел 4.3. Выпуск регистрационных свидетельств

61. Запросы на выпуск регистрационных свидетельств подписываются ЭЦП работников УЦ, имеющих право на их формирование.

62. Запросы на выпуск регистрационных свидетельств для обслуживаемых лиц принимаются только от ИС Банка. Запросы в Центр сертификации из подсистемы облачной ЭЦП подписываются только служебным ключом руководителя УЦ.

63. При обработке запроса на выпуск регистрационного свидетельства УЦ проверяет факт обладания закрытым ключом ЭЦП, соответствующим открытому ключу ЭЦП, на который запрашивается регистрационное свидетельство. Способом доказательства владения закрытым ключом ЭЦП является электронный документ в формате PKCS#10.

64. Официальным уведомлением владельца о выдаче регистрационного свидетельства является его публикация в хранилище УЦ и доступность регистрационного свидетельства в приложении ВСС.

Раздел 4.4. Принятие регистрационных свидетельств

4.4.1. Действия владельца регистрационного свидетельства, означающие его принятие

65. Выполнение всех следующих условий означает принятие выпущенного регистрационного свидетельства его владельцем:

1) согласие выполнять условия Политики регистрационных свидетельств и Регламента, выраженное в заявке на выдачу регистрационного свидетельства;

2) получение регистрационного свидетельства;

3) отсутствие у владельца возражений (претензий) по содержанию регистрационного свидетельства;

4) использование закрытого ключа ЭЦП, соответствующего регистрационному свидетельству.

4.4.2. Публикация регистрационного свидетельства

66. Центр сертификации публикует регистрационное свидетельство в хранилище в соответствии с Регламентом. Публикация регистрационного свидетельства происходит сразу после обработки запроса на его выпуск.

Раздел 4.5. Использование регистрационных свидетельств и ключевых пар

4.5.1. Использование закрытого ключа электронной цифровой подписи и регистрационного свидетельства их владельцем

63. Использование закрытого ключа ЭЦП и регистрационного свидетельства их владельцем допустимо только в соответствии с Политикой регистрационных свидетельств и Регламентом.

64. Первое использование закрытого ключа ЭЦП владельцем регистрационного свидетельства при выполнении остальных условий параграфа 4.4.1 Регламента означает принятие регистрационного свидетельства его владельцем.

65. Владельцы технологических регистрационных свидетельств (служебные пользователи) УЦ обязаны принимать меры для защиты принадлежащих им закрытых ключей ЭЦП от неправомерного доступа и использования в порядке, установленном действующим законодательством Республики Казахстан.

66. УЦ обязан принимать меры для защиты хранимых в HSM закрытых ключей ЭЦП от неправомерного доступа и использования в порядке, установленном Правилами облачной ЭЦП.

4.5.2. Использование регистрационного свидетельства и открытого ключа электронной цифровой подписи доверяющей стороной

67. Регистрационные свидетельства, выданные УЦ, и содержащиеся в них открытые ключи ЭЦП применимы для проверки ЭЦП.

68. Доверяющие стороны должны использовать регистрационные свидетельства строго в соответствии с указанными в них сведениями и Регламентом. Получение дополнительных сведений и гарантий, помимо сведений, указанных в регистрационном свидетельстве, осуществляется доверяющими сторонами самостоятельно.

69. Для проверки и принятия решения о доверии к регистрационному свидетельству, необходимо использовать Правила проверки ЭЦП.

Раздел 4.6. Обновление сроков действия регистрационного свидетельства

70. Обновление регистрационного свидетельства – процедура выпуска регистрационного свидетельства с новыми сроками действия без изменения других данных, указанных в действующем регистрационном свидетельстве.

71. УЦ не выполняет обновления регистрационных свидетельств.

72. В случае необходимости дальнейшей работы владельцу на новый срок действия выпускается регистрационное свидетельство с новым открытым ключом ЭЦП.

Раздел 4.7. Смена ключей электронной цифровой подписи в регистрационном свидетельстве

73. Смена ключей – процедура выпуска регистрационного свидетельства с новым открытым ключом ЭЦП и новыми сроками действия без изменения других данных, указанных в действующем регистрационном свидетельстве. Данная процедура подразумевает изготовление нового закрытого ключа ЭЦП и соответствующего ему регистрационного свидетельства.

74. Смена ключей ЭЦП и регистрационного свидетельства может быть инициирована их владельцем самостоятельно.

75. Процедуры подачи заявки и выпуска регистрационного свидетельства при смене ключей ЭЦП полностью аналогичны процедурам подачи заявки на выдачу регистрационного свидетельства и ее обработки.

Раздел 4.8. Изменение сведений, указанных в регистрационном свидетельстве

76. Изменение сведений, указанных в регистрационном свидетельстве – процедура выпуска регистрационного свидетельства с новыми данными о его владельце без изменения открытого ключа ЭЦП и сроков действия, указанных в действующем регистрационном свидетельстве.

77. УЦ не выполняет изменение сведений, указанных в регистрационных свидетельствах.

78. В случае утраты актуальности сведений, указанных в действующем регистрационном свидетельстве, владелец обязан отозвать регистрационное свидетельство в соответствии с разделом 4.9 Регламента и подать заявку на выдачу нового регистрационного свидетельства в соответствии с разделом 4.1 Регламента.

79. Процедура подачи заявки и выпуска регистрационного свидетельства при изменении указанных в нем сведений, полностью аналогична процедурам подачи заявки на выдачу регистрационного свидетельства и ее обработки.

Раздел 4.9. Отзыв и приостановление действия регистрационного свидетельства

4.9.1. Основания для отзыва регистрационного свидетельства

80. УЦ может отозвать регистрационное свидетельство и опубликовать его в СОРС в следующих случаях:

1) по требованию владельца регистрационного свидетельства;

2) при установлении факта предоставления недостоверных сведений при получении регистрационного свидетельства;

3) смерти владельца регистрационного свидетельства;

4) изменения фамилии, имени или отчества владельца регистрационного свидетельства;

5) предусмотренных соглашением между УЦ и владельцем регистрационного свидетельства;

6) по вступившему в законную силу решению суда.

4.9.2. Лица, имеющие право подавать заявки на отзыв регистрационного свидетельства

81. Заявку на отзыв регистрационного свидетельства может подавать физическое лицо – его владелец или работник ЦР, а для технологических регистрационных свидетельств – работник УЦ.

4.9.3. Процедуры для заявок на отзыв регистрационного свидетельства

82. Подача заявок на **отзыв** регистрационных свидетельств для обслуживаемых физических лиц осуществляется через дистанционный канал (приложение ВСС). Заявка создается в электронном виде, ее форма приведена в приложении 2 к Регламенту. При этом соответствующие запросы в Центр сертификации формируются и обрабатывается автоматически, при условии успешного прохождения заявителем процедур идентификации и аутентификации.

83. Процедуры идентификации и аутентификации заявителя при формировании заявки на отзыв регистрационного свидетельства, подаваемой обслуживаемым лицом или работником ЦР, выполняются в соответствии с требованиями параграфа 3.4.1 Регламента, с применением биометрической аутентификации и идентификации.

84. Подача заявок на отзыв технологического регистрационного свидетельства для служебных пользователей УЦ осуществляется путем личной явки в УЦ, заполнения заявления на отзыв регистрационного свидетельства по форме Правил выпуска и отзыва регистрационных свидетельств и его заверения личной подписью заявителя. Заявки на отзыв регистрационных свидетельств обрабатывают работники УЦ, в соответствии с Правилами выпуска и отзыва регистрационных свидетельств.

85. Процедура идентификации и аутентификации заявителя при обработке заявки на отзыв технологического регистрационного свидетельства, оформленной работником УЦ, выполняется в соответствии с требованиями параграфа 3.4.2 Регламента.

86. В контексте Регламента заявка на отзыв регистрационного свидетельства означает или электронную заявку по форме приложения 2 к Регламенту, или заявление в виде документа на бумажном носителе по форме Правил выпуска и отзыва регистрационных свидетельств.

4.9.4. Срок подачи заявки на отзыв регистрационного свидетельства

87. Лица, имеющие право подавать заявки на отзыв регистрационных свидетельств, обязаны делать это немедленно при первой возможности, как только им становится известно о наступлении оснований, перечисленных в параграфе 4.9.1 Регламента.

4.9.5. Срок обработки заявки на отзыв регистрационного свидетельства

88. Отзыв по заявкам, поданным в отношении регистрационных свидетельств обслуживаемых лиц, осуществляется немедленно.

89. Отзыв регистрационных свидетельств по заявкам, оформленным работником УЦ, осуществляется в срок не более одного рабочего дня.

4.9.6. Требования о необходимости проверки факта отзыва регистрационного свидетельства доверяющей стороной

90. Любой участник ИОК Банка проверяет статус регистрационных свидетельств. Для проверки можно использовать CORC или сервис OCSP. Информация об адресах CORC и сервиса OCSP указана в каждом выпущенном регистрационном свидетельстве и Регламенте. Сервис проверки электронных документов доступен в приложении ВСС и предназначен для получения списка электронных документов, которые подписал владелец регистрационного свидетельства.

4.9.7. Частота выпуска списка отозванных регистрационных свидетельств

91. CORC обновляется при смене статуса любого регистрационного свидетельства, выпущенного УЦ. При выпуске нового CORC из него удаляются отозванные регистрационные свидетельства с истекшим сроком действия.

92. CORC предоставляется в электронной форме в формате, определенном RFC 3280. CORC заверяется ЭЦП Центра сертификации. Доступ к CORC обеспечивается по протоколу HTTP.

4.9.8. Максимальный интервал между выпусками списка отозванных регистрационных свидетельств

93. CORC обновляется не позднее 7 календарных дней с даты подписания предыдущего CORC.

4.9.9. Возможность проверки статуса регистрационного свидетельства в режиме онлайн

94. Информацию о статусе регистрационного свидетельства можно получить, используя сервис службы OCSP.

95. Сервис службы OCSP соответствует требованиям, описанным в RFC 2560. Квитанции с результатом работы сервиса службы OCSP заверяются ЭЦП службы OCSP.

4.9.10. Требование проверки статуса регистрационного свидетельства в режиме онлайн

96. Сервис службы OCSP используется при проверке электронных документов в приложении ВСС.

4.9.11. Другие доступные формы уведомлений об отзыве

97. Других форм уведомления об отзыве регистрационных свидетельств УЦ не предоставляет.

4.9.12. Особые требования в случае компрометации закрытого ключа электронной цифровой подписи

98. В случае обоснованного подозрения о компрометации закрытого ключа ЭЦП владелец соответствующего регистрационного свидетельства выполняет его отзыв согласно разделу 4.9 Регламента и при необходимости подает заявку на выдачу нового регистрационного свидетельства.

4.9.13. Условия приостановления и окончания действия регистрационного свидетельства

99. УЦ не предоставляет услуг временного приостановления действия регистрационных свидетельств.

100. Любое регистрационное свидетельство, выпущенное УЦ, становится недействительным по истечении указанного в нем срока действия.

101. Владелец вправе отозвать регистрационное свидетельство до окончания срока его действия в соответствии с разделом 4.9 Регламента.

102. Отозванные регистрационные свидетельства хранятся в УЦ в течение всего периода работы УЦ, но не менее пяти лет.

103. В случае прекращения деятельности УЦ отозванные регистрационные свидетельства подлежат дальнейшему хранению в Банке соответствии с законодательством Республики Казахстан[4] или передаются по согласованию с их владельцем в другой удостоверяющий центр.

Глава 5. ФИЗИЧЕСКИЙ, ОПЕРАЦИОННЫЙ И УПРАВЛЯЮЩИЙ КОНТРОЛЬ

Раздел 5.1. Физический контроль

103. ИС УЦ, обрабатывающая запросы участников ИОК, расположена в специализированных центрах обработки данных.

104. Физический доступ в основной и резервный центры обработки данных организованы и контролируются одинаковыми мерами безопасности. Серверные помещения 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.

105. УЦ ведет архив в соответствии с действующим внутренним документом Банка, регламентирующим резервное копирование и восстановление информации.

106. Утилизация носителей конфиденциальных данных УЦ осуществляется в соответствии с действующим внутренним документом Банка, регламентирующем уничтожение информации на технических носителях.

Раздел 5.2. Операционный контроль

107. В целях операционного контроля полномочия работников УЦ и участников ИОК разбиты на 3 следующие категории (роли):

1) администратор УЦ;
2) аудитор УЦ;
3) пользователь УЦ.

[4] Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи», ст. 22, п.4.

Раздел 5.3. Контроль персонала

5.3.1. Требования к квалификации персонала

108. Перед назначением на должности в УЦ соискатели предоставляют документы, определенные Трудовым кодексом Республики Казахстан, и проходят скрининг в соответствии с внутренним документом Банка по подбору персонала.

5.3.2. Процедура проверки работников

109. Проверка работников осуществляется в соответствии с внутренними инструкциями Центра обеспечения безопасности Банка.

5.3.3. Требования к обучению персонала

110. Комплектование штата работников УЦ осуществляется специалистами профильного (технического, математического, ИТ) образования.

5.3.4. Требования к повышению квалификации персонала

111. Специалисты и руководители УЦ проходят обучение или сертификацию не реже одного раза в три года.

5.3.5. Частота и последовательность смены деятельности работников

112. Не определено.

5.3.6. Ответственность за нарушения

113. Персонал УЦ и ЦР несет ответственность за свои действия в соответствии с внутренними нормативными документами Банка и действующим законодательством Республики Казахстан.

5.3.7. Требования к независимым подрядчикам

114. В исключительных случаях, когда для выполнения работ требуются услуги независимых подрядчиков, специалисты подрядчиков проводят работы только под наблюдением и с разрешения работников УЦ.

5.3.8. Документация, предоставляемая персоналу

115. Деятельность работников УЦ регламентирована должностными инструкциями и внутренними нормативными документами Банка.

116. Доступ работников УЦ к документальному фонду организован в соответствии с должностными инструкциями и функциональными обязанностями.

Раздел 5.4. Процедуры контрольного протоколирования и управления инцидентами информационной безопасности

5.4.1. Типы событий, подлежащих аудиту

117. УЦ обеспечивает протоколирование следующих событий:

1) запрос на выпуск регистрационного свидетельства;
2) запрос на отзыв регистрационного свидетельства;
3) формирование закрытого ключа ЭЦП облачной ЭЦП;
4) использование закрытого ключа ЭЦП облачной ЭЦП;
5) удаление (стирание) закрытого ключа ЭЦП облачной ЭЦП.

118. Срок хранения протоколов работы составляет один год с даты истечения срока действия регистрационного свидетельства.

119. При протоколировании действий записывается следующая информация:

1) дата, время;

2) DN владельца регистрационного свидетельства;
3) тип события.

5.4.2. Частота анализа журналов аудита

120. Журналы аудита ежедневно анализируются работниками УЦ с целью обнаружения ошибок и нарушений в работе программного и аппаратного обеспечения Центра сертификации, анализа производительности систем, а также по мере регистрации инцидентов от ИС, использующих УЦ.

5.4.3. Срок хранения журналов аудита

121. Срок хранения архива журналов аудита определяется в соответствии с требованиями Правил облачной ЭЦП.

5.4.4. Защита журналов аудита

122. Протоколы событий ежедневно преобразуется в хэш, и данные хэш хранятся в цепочке событий блокчейн. Мониторинг системы блокчейн доступен в сети Интернет по ссылке: http://91.147.113.4:4000/

5.4.5. Резервное копирование журналов аудита

123. Журналы аудита подлежат резервному копированию ежесуточно, с возможностью восстановления из резервной копии и проверки целостности.

5.4.6. Условия сбора данных для аудита

124. События аудита автоматически записываются в журналы средствами прикладного и общесистемного программного обеспечения.

5.4.7. Уведомление субъекта события, вносимого в журнал аудита

125. При записи события в журнал аудита уведомление субъекта этого события не требуется.

5.4.8. Анализ несоответствий и управление инцидентами информационной безопасности

126. Процесс управления инцидентами информационной безопасности осуществляется в соответствии внутренним нормативным документом Банка по вопросам управления инцидентами информационной безопасности.

Раздел 5.5. Ведение архива

5.5.1. Типы регистрируемых событий

127. УЦ ведет архив:
1) журналов аудита в соответствии с разделом 5.4 Регламента;
2) регистрационных свидетельств пользователей УЦ, срок действия которых истек;
3) отозванных регистрационных свидетельств пользователей УЦ;
4) CORC;
5) протоколов работы программного обеспечения УЦ.

5.5.2. Срок хранения архива

128. УЦ хранит архив на протяжении всего срока работы.

5.5.3. Защита архива

129. УЦ обеспечивает хранение архивных документов в соответствии с законодательством Республики Казахстан.

5.5.4. Условия архивирования

130. УЦ обеспечивает ведение архива в соответствии с законодательством Республики Казахстан.

5.5.5. Требования к простановке времени создания архивных записей

131. Не определено.

5.5.6. Система сбора архива

132. Архивные копии данных УЦ записываются на выделенные для этой цели дисковые или ленточные системы хранения данных, управляемые ответственным подразделением ИТ Банка.

5.5.7. Порядок получения и проверки информации, хранящейся в архиве

133. Доступ к архиву УЦ имеют только администраторы УЦ.

Раздел 5.6. Смена ключей электронной цифровой подписи Центра сертификации

134. Заблаговременно до окончания срока действия закрытого ключа ЭЦП Центра сертификации, администратор УЦ производит формирование нового закрытого ключа ЭЦП и регистрационного свидетельства Центра сертификации и публикует регистрационное свидетельство в соответствующий раздел хранилища.

135. По окончании действия закрытого ключа ЭЦП Центра сертификации его резервные копии уничтожаются по акту.

Раздел 5.7. Восстановление функционирования в случае компрометации или сбоев

5.7.1. Действия по предотвращению компрометации и сбоев

136. Для предотвращения потери данные Центра сертификации (хранилище, ключи Центра сертификации) архивируются и помещаются в специально предназначенные для этих целей хранилища.

5.7.2. Случаи повреждения оборудования, программных и/или аппаратных сбоев

137. В случае повреждения оборудования, программных и/или аппаратных сбоев, сведения о происшествии поступают к руководству Центра сертификации, которое расследует происшествие и принимает необходимые меры по устранению последствий и недопущению повторения подобных инцидентов.

138. Восстановительные работы проводятся в соответствии с внутренним планом восстановления УЦ.

5.7.3. Компрометация закрытого ключа электронной цифровой подписи участника информационной системы

139. В случае если есть основания полагать, что пароль к закрытому ключу ЭЦП стал доступен третьим лицам, требуется немедленно направить в УЦ запрос на отзыв регистрационного свидетельства.

5.7.4. Восстановление работоспособности после аварии

140. Случаи повреждения вычислительных, программных ресурсов и/или данных ИС УЦ обрабатываются в соответствии с внутренним нормативным документом Банка, устанавливающим порядок действий работников УЦ в нештатных и кризисных ситуациях.

5.7.5. Разрешение конфликтных ситуаций (непризнание электронной цифровой подписи электронного документа, его целостности и подлинности)

141. Споры между участниками ИОК: между владельцами регистрационных свидетельств и доверяющими сторонами, а также между владельцем регистрационного свидетельства или доверяющей стороной, с одной стороны, и УЦ или ЦР, с другой стороны, – разрешаются в соответствии с положениями законодательства Республики Казахстан и договоров, действующих между сторонами (при наличии).

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

143. Для разрешения споров, предметом которых являются разногласия по существу Регламента, применяется законодательство Республики Казахстан.

5.7.6. Процедура проверки электронной цифровой подписи документа

144. Процедура проверки ЭЦП электронного документа включает в себя проверку действительности регистрационного свидетельства на момент подписания и проверку соответствия сведениям в регистрационном свидетельстве, с использованием Правил проверки ЭЦП.

Раздел 5.8. Прекращение работы Удостоверяющего центра

145. В случае принятия решения о прекращение работы УЦ уведомление владельцев регистрационных свидетельств, передача и архивное хранение записей УЦ организовываются в соответствии со ст. 22 Закона Республики Казахстан «Об электронном документе и электронной цифровой подписи».

Глава 6. ТЕХНИЧЕСКИЙ КОНТРОЛЬ БЕЗОПАСНОСТИ

Раздел 6.1. Изготовление и установка ключевых пар электронной цифровой подписи

6.1.1. Изготовление ключей электронной цифровой подписи и используемые алгоритмы

146. Создание закрытых ключей ЭЦП Центра сертификации проводится администратором УЦ Банка.

147. Ключи ЭЦП Центра сертификации формируются на электронных НКИ в сертифицированном HSM и не могут быть извлечены из него в незащищенном виде.

148. Закрытые ключи ЭЦП владельцев регистрационных свидетельств, хранящиеся в облачной ЭЦП, создаются строго внутри HSM. Закрытый ключ ЭЦП облачной ЭЦП не извлекается из HSM в открытом виде.

149. Требования к HSM облачной ЭЦП:

1) не ниже третьего уровня безопасности в соответствии с требованиями Стандарта;

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 Республики Казахстан.

150. Все ключи ЭЦП формируются в соответствии с алгоритмом ГОСТ 34.310–2004.

6.1.2. Передача закрытого ключа электронной цифровой подписи владельцу регистрационного свидетельства

151. Использование закрытых ключей ЭЦП, создаваемых внутри HSM облачной ЭЦП, владельцами соответствующих им регистрационных свидетельств осуществляется только внутри этих же HSM. Физическая передача копий указанных закрытых ключей ЭЦП их владельцам не предусмотрена.

152. Закрытые ключи ЭЦП, соответствующие технологическим регистрационным свидетельствам УЦ, выдаются владеющим ими работникам УЦ как правило только на НКИ. В исключительных случаях, когда отсутствует техническая возможность использовать такой технологический закрытый ключ непосредственно с НКИ, допускается после генерации сохранять его на незащищенный носитель информации, но с обязательным использованием данных активации в форме пароля.

6.1.3. Передача открытых ключей электронной цифровой подписи доверяющим сторонам

153. УЦ публикует регистрационные свидетельства и СОРС в соответствии с порядком, описанным в Регламенте.

154. При выпуске своего регистрационного свидетельства участник ИС имеет возможность ознакомиться с Политикой регистрационных свидетельств и Регламентом. Ознакомившись с указанными документами и отправляя заявку на выдачу регистрационного свидетельства, пользователь подтверждает свое полное и безоговорочное согласие с условиями использования сервисов УЦ.

6.1.4. Доставка открытого ключа УЦ доверяющим сторонам

155. Предоставление открытого ключа Центра сертификации реализовано посредством публикации его регистрационного свидетельства на официальном информационном ресурсе Банка в сети Интернет по адресу https://www.bcc.kz/product/pki/docs/CA_GOST.cer?v=2.0.0.

6.1.5. Размеры ключей электронной цифровой подписи

156. При использовании схемы ЭЦП по алгоритму ГОСТ 34.310–2004 длина: закрытого ключа составляет 256 двоичных разрядов, открытого ключа – 512 двоичных разрядов.

6.1.6. Генерация и проверка качества параметров открытого ключа электронной цифровой подписи

157. Параметры генерации и проверки качества параметров ключей ЭЦП определяются СКЗИ, сертифицированным в соответствии со Стандартом, автоматически.

6.1.7. Цели использования ключей электронной цифровой подписи

158. Значения в расширении «Key Usage» регистрационных свидетельств обслуживаемых владельцев:

1) цифровая подпись;
2) неотрекаемость.

6.1.8. Требования к носителям ключевой информации

159. УЦ поддерживает применение электронных НКИ и имеет техническую возможность работы со следующими НКИ:

1) CERTEX HSM;
2) CERTEX HSM ES;
3) SafeNet 5100;
4) SafeNet 5110;
5) KAZTOKEN;
6) KAZTOKEN смарт-карта.

Раздел 6.2. Защита закрытого ключа электронной цифровой подписи и инженерные контроли аппаратных криптографических модулей

160. Резервное копирование закрытого ключа ЭЦП пользователя не предусмотрено.

161. Резервное копирование закрытого ключа ЭЦП Центра сертификации происходит в соответствии с эксплуатационной документацией HSM по схеме m из n. Резервная копия закрытого ключа Центра сертификации хранится отдельно от HSM в зашифрованном архиве.

162. Закрытые ключи с истекшим сроком действия подлежат уничтожению в соответствии с эксплуатационной документацией СКЗИ. Архивное хранение закрытых ключей ЭЦП не допускается.

163. После создания закрытый ключ ЭЦП облачной ЭЦП сохраняется в HSM в зашифрованном виде с использованием стандарта ГОСТ 28147–89. В качестве секретных значений используется пароль, который в УЦ не хранится.

164. Запись закрытого ключа ЭЦП облачной ЭЦП в HSM производится штатными средствами HSM в соответствии с эксплуатационной документацией HSM.

165. Закрытые ключи ЭЦП облачной ЭЦП хранятся только в зашифрованном виде и не покидают HSM иначе как в зашифрованном архиве.

Раздел 6.3. Другие особенности управления ключами электронной цифровой подписи

6.3.1. Архивирование открытых ключей электронной цифровой подписи

166. Все регистрационные свидетельства архивируются в соответствии с порядком резервного копирования, установленным в УЦ.

6.3.2. Сроки действия регистрационных свидетельств и ключей электронной цифровой подписи

167. Начало периода действия регистрационного свидетельства Центра сертификации исчисляется с даты и времени его выпуска. Срок действия корневого регистрационного свидетельства УЦ составляет 20 лет.

168. Срок действия регистрационного свидетельства обслуживаемых УЦ физических лиц, составляет один календарный год. Начало периода действия закрытого ключа ЭЦП владельца регистрационного свидетельства исчисляется с даты и времени начала действия соответствующего регистрационного свидетельства.

6.3.3. Ограничения на использования ключей электронной цифровой подписи

169. Закрытый ключ ЭЦП Центра сертификации используется для формирования ЭЦП в регистрационных свидетельствах открытых ключей ЭЦП их владельцев, а также в СОРС.

170. Закрытые ключи ЭЦП обслуживаемых УЦ физических лиц используются для формирования ЭЦП и подписания электронных документов в ИС Банка.

171. В случае смены ключей ЭЦП Центра сертификации и выпуска нового регистрационного свидетельства Центра сертификации его внедрение может производиться с использованием механизма кросс-сертификации.

Раздел 6.4. Данные активации

6.4.1. Генерация и установка данных активации

172. При установке пароля на закрытый ключ ЭЦП обслуживаемое УЦ физическое лицо обязано создать пароль, при этом пароль должен содержать:

1) латинские буквы, в верхнем и нижнем регистре;
2) минимум одну цифру;
3) минимум один спецсимвол;
4) минимум 8 символов.

6.4.2. Защита данных активации

173. Запрещается записывать пароль доступа к закрытому ключу ЭЦП. Пароль должен быть известен только владельцу соответствующего регистрационного свидетельства. Запрещается использование функции автоматического сохранения пароля в используемых средствах безопасности.

Раздел 6.5. Контроль безопасности вычислительных ресурсов

174. Требования к серверам ИОК:

1) обеспечение мер отказоустойчивости и безопасности;

2) ежегодное сканирование безопасности;

3) мониторинг ресурсов.

175. Компьютеры администраторов УЦ должны удовлетворять следующим требованиям:

1) использование лицензионного программного обеспечения;

2) операционные системы поддерживаются на высоком уровне защиты, при регулярном применении всех рекомендованных и соответствующих пакетов защиты, в том числе антивирусов и межсетевых экранов;

3) недопустимость совместного использования компьютера несколькими пользователями;

4) на компьютере отсутствуют СКЗИ, отличные от определенных в Регламенте.

176. Схема взаимодействия модулей УЦ приведена в приложении 3 к Регламенту.

177. Безопасность аппаратных средств Центра сертификации обеспечивается антивирусами и межсетевыми экранами.

Глава 7. ПРОФИЛИ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ, СПИСКОВ ОТОЗВАННЫХ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ И СЕРВИСА ПРОТОКОЛА ПРОВЕРКИ СТАТУСА РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ В РЕЖИМЕ ОНЛАЙН

Раздел 7.1. Профили регистрационных свидетельств

178. Центр сертификации выдает регистрационные свидетельства, соответствующие рекомендациям X.509 ITU-T версии 3 и RFC 3280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile».

179. Центр сертификации для идентификации криптографических алгоритмов использует OID Республики Казахстан https://root.gov.kz/oid/.

180. Схемы ЭЦП с описанием применяемых криптографических алгоритмов приведены в приложении 4 к Регламенту.

181. В регистрационные свидетельства пользователей ИС Банка – их владельцев включается OID политики пользователя ИС "ВСС KZ" – 1.2.398.3.24.3.2.2.

182. Структура регистрационного свидетельства УЦ

Название	Содержание
Версия	V3
Серийный номер	5cd5f1cb8b17936fbe05c2b9ab59174331c8557a
Алгоритм подписи	ГОСТ 34.310
Поставщик	CN = Certification Authority O = Bank CenterCredit JSC C = KZ
Субъект	CN = Certification Authority O = Bank CenterCredit JSC C = KZ
Действителен с	16 октября 2023 г. 9:47:55
Действителен по	16 октября 2043 г. 9:47:55
Алгоритм открытого ключа	ГОСТ 34.310 (512 Bits)
Открытый ключ	04 40 ec 88 2d cf d7 e1 b5 c7 70 5c 66 15 35 a7 dc 78 c7 bf dd cb 09 7c 8b 6c 95 e3 29 f9 ed b1 93 80 b1 65 9e 3d d1 0c 06 13 7c c9 0c 0c ad 9e ff 4f d3 ff 97 30 c6 1f 2a 19 01 e1 56 6c 0d e8 30 81
Идентификатор ключа	5cd5f1cb8b17936fbe05c2b9ab59174331c8557a
Политика сертификата	1.2.398.3.24.1.1.1
Использование ключа	Подписывание сертификатов Автономное подписание списка отзыва (CRL) Подписывание списка отзыва (CRL)

Название	Содержание
Подпись	ЭЦП

183. Структура технологических регистрационных свидетельств работников Банка

Название	Содержание
Версия	V3
Серийный номер	
Алгоритм подписи	ГОСТ 34.310
Поставщик	CN = Certification Authority O = Bank CenterCredit JSC C = KZ
Субъект	[UID = IIN1111111111111] CN=BIN123456789012 или CN=*имя службы УЦ* [OU=Certification Authority] O = Bank CenterCredit JSC C = KZ
Действителен с	
Действителен по	
Алгоритм открытого ключа	ГОСТ 34.310 (512 Bits)
Открытый ключ	
Идентификатор ключа	
Идентификатор ключа УЦ	5cd5f1cb8b17936fbe05c2b9ab59174331c8557a
Политика сертификата	1.2.398.3.24.1.1.1
Использование ключа	Цифровая подпись Неотрекаемость
Подпись	ЭЦП

184. Структура регистрационного свидетельства обслуживаемого УЦ физического лица

Название	Содержание
Версия	V3
Серийный номер	
Алгоритм подписи	ГОСТ 34.310
Поставщик	C = KZ O = Bank CenterCredit JSC CN = Certification Authority
Субъект	UID = IIN1111111111111 OU=BCC.KZ O = Bank CenterCredit JSC C = KZ
Действителен с	
Действителен по	
Алгоритм открытого ключа	ГОСТ 34.310–2004 (512 Bits)
Открытый ключ	
Идентификатор ключа	
Идентификатор ключа УЦ	5cd5f1cb8b17936fbe05c2b9ab59174331c8557a
Политика сертификата	1.2.398.3.24.1.1.1 1.2.398.3.24.3.2.2
Использование ключа	Цифровая подпись Неотрекаемость
Подпись	ЭЦП

Раздел 7.2. Профиль списка отозванных регистрационных свидетельств

Название	Содержание
Версия	V2
Издатель	CN = Certification Authority O = Bank CenterCredit JSC C = KZ
Действителен с	
Следующее обновление	
Алгоритм подписи	ГОСТ 34.310
Идентификатор ключа УЦ	5cd5f1cb8b17936fbe05c2b9ab59174331c8557a
Список отзыва	Серийный номер Дата отзыва Код причины списка отзыва

Раздел 7.3. Профиль сервиса протокола проверки статуса регистрационных свидетельств в режиме онлайн

185. OCSP может использоваться доверяющими сторонами для определения статуса конкретного указанного регистрационного свидетельства в текущий момент времени.

186. УЦ формирует квитанции OCSP в электронной форме по версии 1 в соответствии с RFC 2560 «Online Certificate Status Protocol – OCSP».

Глава 8. ПРОВЕРКА ДЕЯТЕЛЬНОСТИ

187. Аккредитация УЦ осуществляется сроком на три года[5] в соответствии с законодательством Республики Казахстан[6].

188. Кроме этого, деятельность Центра обеспечения информационной безопасности, в состав которого входит УЦ, на плановой основе подвергается внутреннему аудиту в соответствии с внутренним документом Банка.

Глава 9. ВОПРОСЫ ТАРИФИКАЦИИ И ОТВЕТСТВЕННОСТИ

Раздел 9.1. Тарифы

189. Услуги УЦ не тарифицируются и не оплачиваются.

Раздел 9.2. Ответственность

190. Ответственность участников ИОК, обслуживаемой УЦ, установлена законодательством Республики Казахстан[7].

191. Ответственность персонала УЦ и ЦР установлена трудовым договором и должностными инструкциями.

Глава 10. ПРОЧИЕ ВОПРОСЫ

Раздел 10.1. Разрешение споров

192. Для разрешения споров, предметом которых являются разногласия по существу Регламента, применяется законодательство Республики Казахстан.

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

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

---

[5] Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи», статья 20-2.

[6] На дату утверждения Регламента действуют Правила выдачи и отзыва свидетельства об аккредитации удостоверяющих центров в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 30 сентября 2022 года № 363/НҚ.

[7] Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи», статья 20-2.

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

Раздел 10.2. Гарантии и заверения

196. УЦ обеспечивает:

1) соответствие данных, содержащихся в выпущенных им регистрационных свидетельствах, тем сведениям, которые предоставил ЦР 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 персонала УЦ;

2) соответствие оказываемых услуг (выпуск, отзыв регистрационных свидетельств, выпуск CORC, онлайн-сервисы OCSP и TSP, создание и защищенное хранение закрытых ключей ЭЦП, формирование ЭЦП по запросам владельца регистрационных свидетельств) требованиям: действующего законодательства Республики Казахстан по вопросам электронного документа и электронной цифровой подписи, Политики регистрационных свидетельств и Регламента;

3) публикацию требований Политики регистрационных свидетельств и Регламента на официальном информационном ресурсе Банка в сети Интернет.

197. ЦР обеспечивают:

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

2) соответствие выполняемых персоналом ЦР процедур (регистрация и обработка заявок на выдачу и отзыв регистрационных свидетельств, процедуры идентификации и аутентификации заявителей, выдача регистрационных свидетельств их владельцам) требованиям: действующего законодательства Республики Казахстан по вопросам электронного документа и электронной цифровой подписи, Политики регистрационных свидетельств и Регламента.

Раздел 10.3. Отказ от гарантий и ограничение ответственности

198. Участники ИОК не несут ответственности за непрямой, особый, случайный или вытекающий ущерб и упущенную выгоду.

199. УЦ не несет перед владельцами регистрационных свидетельств 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.

Раздел 10.4. Вступление в силу и прекращение действия

200. Регламент и все изменения и дополнения к нему вступают в силу не ранее дня опубликования на официальном ресурсе Банка в сети Интернет.

201. Регламент, с учетом публикуемых изменений и дополнений к нему, сохраняет силу до момента опубликования своей новой редакции на официальном ресурсе Банка в сети Интернет.

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

Раздел 10.5. Защита персональных данных участников инфраструктуры открытых ключей

203. УЦ обеспечивает защиту персональных данных участников ИОК в соответствии с законодательством Республики Казахстан по вопросам персональных данных и их защиты.

204. Форма заявки на выдачу регистрационного свидетельства подтверждает согласие заявителя на сбор, обработку и хранение его персональных данных в соответствии с законодательством

Республики Казахстан по вопросам персональных данных и их защиты[8], в том числе дает УЦ разрешение на публикацию регистрационных свидетельств заявителя и информации об их статусе в хранилище.

Раздел 10.6. Отдельные аспекты прав собственности

205. Любое выпущенное УЦ регистрационное свидетельство и содержащийся в нем открытый ключ ЭЦП являются собственностью Банка. При этом заявитель, который принял выпущенное на его имя регистрационное свидетельство в порядке, изложенном в разделе 4.4 Регламента, автоматически наделяется правом владения этим регистрационным свидетельством и открытым ключом ЭЦП.

206. Доверяющие стороны автоматически наделяются правом пользования любым регистрационным свидетельством и содержащимся в нем открытым ключом ЭЦП с момента их публикации в УЦ.

207. УЦ не запрещает владельцам регистрационных свидетельств и доверяющим сторонам копирование и распространение регистрационных свидетельств, выпущенных УЦ, на неисключительной бесплатной основе, при соблюдении условий полноты и целостности их данных.

208. Закрытый ключ ЭЦП, который соответствует регистрационному свидетельству, выпущенному УЦ, является собственностью владельца этого регистрационного свидетельства.

Раздел 10.7. Компенсации

209. Расходы, связанные с компенсацией за:

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

2) непреднамеренное или умышленное сокрытие существенных фактов, подлежащих отражению в заявках на выдачу или отзыв регистрационного свидетельства, –

в части, не противоречащей действующему законодательству Республики Казахстан, относятся на счет ЦР.

Раздел 10.8. Заключительные положения

210. Требования Регламента обязательны для исполнения всеми работниками подразделений Банка, задействованных в процессах, описанных в Регламенте.

211. Подразделения Банка, взаимодействующие с УЦ, несут ответственность:

1) за соблюдение требований, описанных в Регламенте;

2) за полноту и своевременность исполняемых функций в рамках своих полномочий.

212. Все вопросы, не урегулированные Регламентом, разрешаются в порядке, определенном действующим законодательством Республики Казахстан, иными нормативными документами и решениями уполномоченных органов Банка.

213. Регламент подлежит пересмотру по мере необходимости. Ответственным подразделением за пересмотр и актуализацию Регламента является Дирекция криптографической защиты информации Банка.

Дирекция криптографической защиты информации

[8] Закон Республики Казахстан «О персональных данных и их защите», статья 8.

Приложение 1
к Регламенту деятельности удостоверяющего центра АО «Банк ЦентрКредит»

ЗАЯВЛЕНИЕ
на выдачу регистрационного свидетельства от физического лица

Индивидуальный идентификационный номер: _____

Фамилия: _____
Имя: _____
Отчество: _____
Наименование области: _____
Город: _____
Адрес электронной почты: _____
Телефон: _____

Срок действия регистрационных свидетельств: _____
Информация о сферах применения и ограничениях применения электронной цифровой подписи _____
Данные о средствах электронной цифровой подписи, используемых для создания соответствующего закрытого ключа электронной цифровой подписи, обозначение стандарта алгоритма электронной цифровой подписи и длины открытого ключа: _____
Открытый ключ электронной цифровой подписи: _____
_____

Настоящим подтверждаю, что:

1. С Политикой применения регистрационных свидетельств и Регламентом деятельности удостоверяющего центра (https://www.bcc.kz/product/pki/?tab=DPP) ознакомлен. Обязуюсь выполнять требования указанных документов, включая гарантии и заверения владельца и пользователя регистрационных свидетельств.
2. Согласен на сбор, хранение и обработку моих персональных данных. Документ о согласии подписал.
3. Согласен на хранение своего закрытого ключа ЭЦП в облачной ЭЦП удостоверяющего Центра.

Дата "___" _____ 20____ года
Подпись физического лица _____

Приложение 2
к Регламенту деятельности удостоверяющего центра АО «Банк ЦентрКредит»

ЗАЯВЛЕНИЕ
на отзыв регистрационного свидетельства от физического лица

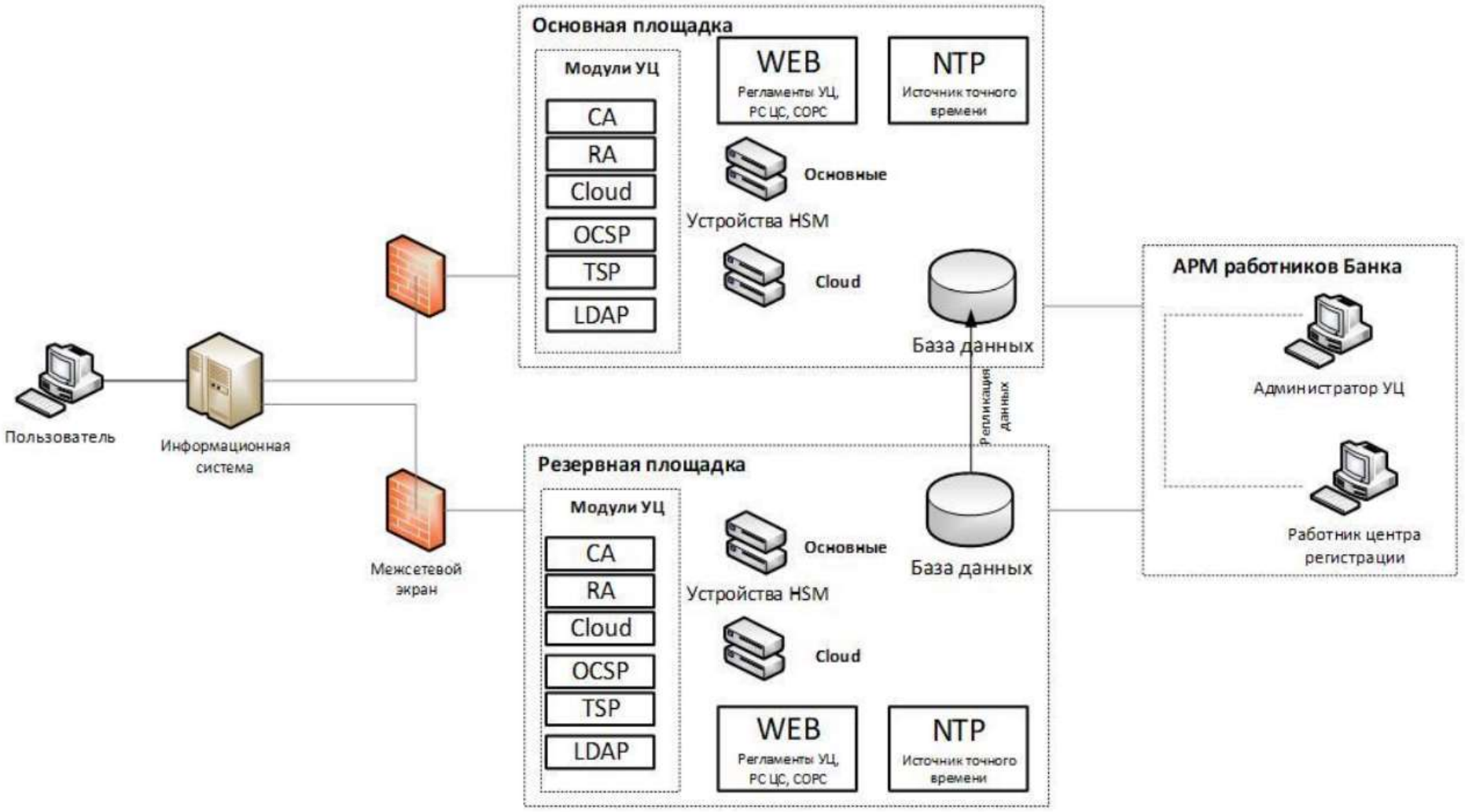
Индивидуальный идентификационный номер: _____
Фамилия: _____
Имя: _____
Отчество: _____
Наименование области: _____
Город: _____
Адрес электронной почты: _____
Телефон: _____

Идентификационные данные регистрационного свидетельства:
Серийный номер:
_____
_____
_____
_____
_____
_____

Дата "___" _____ 20____ года
Подпись физического лица _____

Приложение 3
к Регламенту деятельности удостоверяющего центра АО «Банк ЦентрКредит»

Схема взаимодействия модулей (компонент) удостоверяющего центра



ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к Схеме взаимодействия модулей (компонентов) удостоверяющего центра

Взаимодействие компонентов (основной и резервный центр)

Взаимодействие модулей информационной системы удостоверяющего центра (далее – УЦ) с хранилищем для публикации и поиска регистрационных свидетельств, списков отозванных регистрационных свидетельств 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 второму уровню безопасности согласно СТ РК 1073-2007.

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

Для создания, хранения и обеспечения безопасности закрытых ключей владельцев регистрационных свидетельств используются защищенные программно-аппаратные комплексы HSM, соответствующие 3 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 MySQL и 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 УЦ

Пользователи УЦ напрямую с сервисами УЦ не взаимодействуют.

Взаимодействие осуществляется через целевые (обслуживаемые) информационные системы Банка, которые имеют возможность взаимодействия подсистемой облачной ЭЦП УЦ с использованием протоколов HTTP(S).

Взаимодействие работников УЦ с модулями УЦ

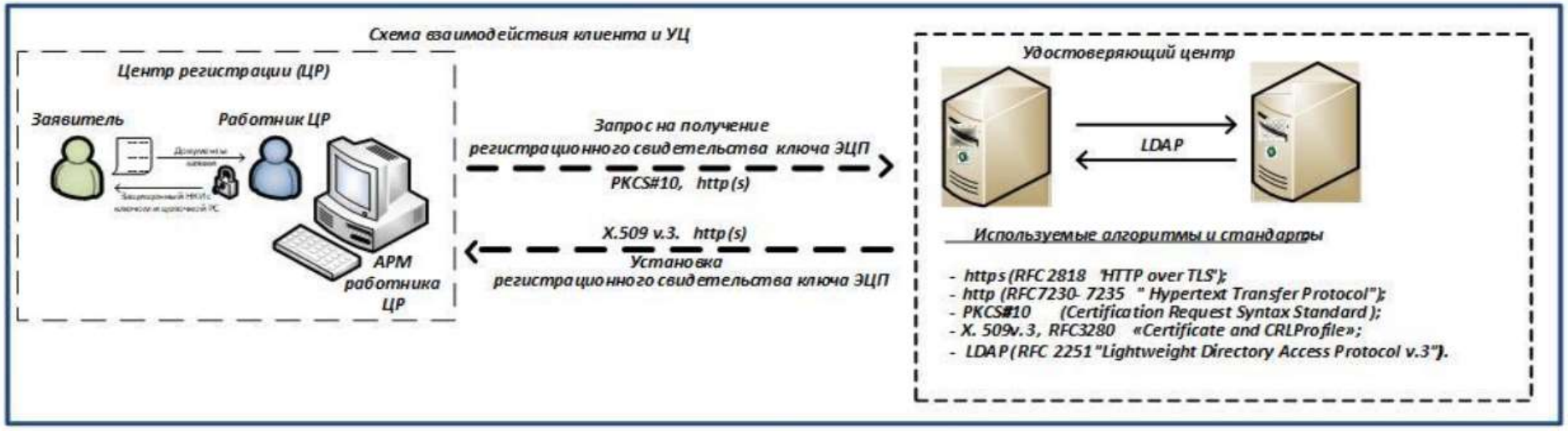
Взаимодействие работников УЦ с модулями УЦ осуществляется посредством специализированного программного обеспечения с использованием протоколов LDAP и HTTP(S).

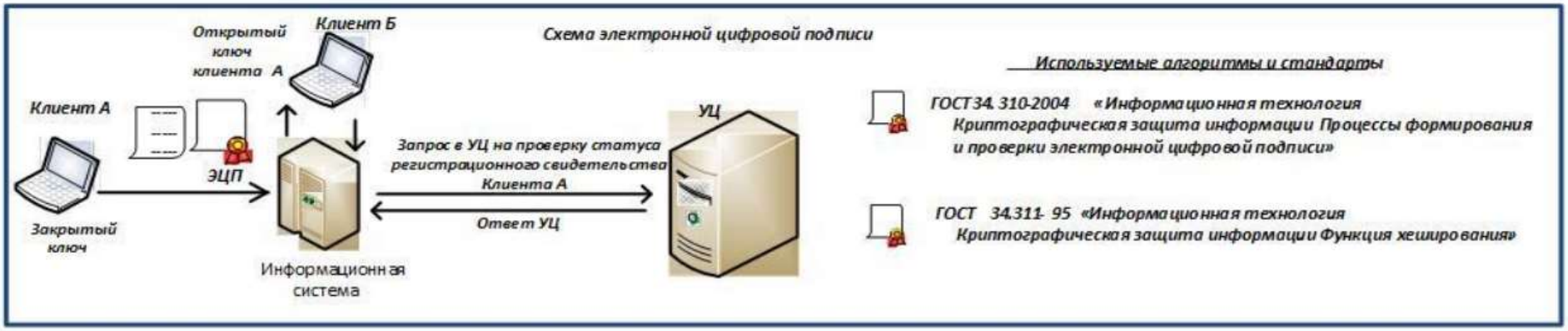
Доступ с рабочего места сотрудника к модулям УЦ возможен только при наличии действующего регистрационного свидетельства с определенными свойствами.

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

Приложение 4
к Регламенту деятельности удостоверяющего центра АО «Банк ЦентрКредит»

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 паратметрам и удостоверяющему центру





Схемы электронной цифровой подписи ... (продолжение)

Особенности процессов при хранении и использовании закрытых ключей владельцев регистрационных свидетельств на стороне Удостоверяющего центра