ВНУТРЕННИЙ ДОКУМЕНТ	
Наименование:	Регламент деятельности удостоверяющего центра АО «Фридом Банк Казахстан»
Владелец:	Департамент информационной безопасности
Утвержден:	Решением Правления (Протокол №97от 20.08.2024г.)
Срок введения в действие:	20.08.2024
Внесение последних изменений/дополнений	Изменение и дополнения в Регламент деятельности удостоверяющего центра ОА «Фридом Банк Казахстан», утвержденные решением Правления №5 от 20.01.2026г.
Отмененные/признанные утратившими силу документы (при наличии):	
Степень конфиденциальности:	Общедоступный

ОГЛАВЛЕНИЕ

РЕЕСТР

утвержденных изменений и дополнений в
Регламент деятельности удостоверяющего центра АО «Фридом Банк Казахстан»

№	Номер документа	Реквизиты решения Органа Банка об утверждении изменений и дополнений	Срок введения в действие утвержденных изменений и дополнений	Основание внесения изменений/дополнений
1	№А0-08-13/197/РГ/20082024	решением Правления №5 от 20.01.2026г	21.01.2026	Изменения и дополнения для устранения замечаний уполномоченного органа
2				
3				
4				
5				
6				

ГЛАВА 1. ОБЩЕЕ ПОЛОЖЕНИЯ

1. Настоящий Регламент деятельности удостоверяющего центра АО «Фридом Банк Казахстан» (далее – Регламент) определяет порядок предоставления услуг Удостоверяющим центром АО «Фридом Банк Казахстан» (далее – УЦ).

2. Регламент является соглашением, налагающим обязательства на все вовлеченные стороны, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

3. Регламент подготовлен в соответствии с рекомендациями RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

4. Регламент разработан в соответствии с Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи» и «Правилами 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», утвержденными приказом Министра по инвестициям и развитию РК от 23 декабря 2015 года № 1231.

РАЗДЕЛ 1. ОБЗОР

5. Регламент определяет правила, механизмы и условия предоставления и использования услуг УЦ, включая права, обязанности и ответственность участников УЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия.

6. Конкретный порядок, особенности отношений УЦ и Заявителей по вопросам, регламентируемым настоящим Регламентом, юридические требования, ответственность Владельцев регистрационных свидетельств при использовании регистрационных свидетельств определяются в договорах (соглашениях), заключаемых с УЦ, внутренними нормативными документами УЦ, устанавливающими особенности предоставления услуг УЦ на основании электронных документов.

РАЗДЕЛ 2. ИСПОЛЬЗУЕМЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

7. Основные понятия и сокращения, используемые в настоящем Регламенте:

1) OTP-пароль (One Time Password, одноразовый пароль) – уникальная последовательность электронных цифровых символов, создаваемая программно-техническими средствами по запросу клиента и предназначенная для одноразового использования при предоставлении доступа клиенту к электронным банковским услугам;

2) Аппаратный криптографический модуль (Hardware Security Module) (далее - HSM) - программно-аппаратный модуль, предназначенный для генерации, хранения, защиты и управления ключами УЦ, закрытыми ключами ЭЦП пользователей;

3) Аутентификация – процесс проверки того, что лицо или предмет является тем, кем (чем) себя объявляет;

4) Банк – АО «Фридом Банк Казахстан»;

5) БИН – бизнес-идентификационный номер;

6) Биометрическая аутентификация – комплекс мер, идентифицирующих личность на основании физиологических и неизменных биологических признаков;

7) Владелец регистрационного свидетельства (далее – Владелец) - физическое лицо или уполномоченный представитель юридического лица, на имя которого выдано

регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве;

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

9) Заявитель – физическое лицо или юридическое лицо, подавшее документы на выдачу или отзыв регистрационного свидетельства;

10) Заявление выдаче регистрационных свидетельств – документ, на основании которого выдается регистрационное свидетельство, составленный по форме Приложения №1 настоящего Регламента;

11) ИИН – индивидуальный идентификационный номер;

12) Компрометация закрытого ключа – утрата доверия к тому, что используемые закрытые ключи не доступны посторонним лицам;

13) 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);

14) Неотрекаемость – невозможность отказа отправителя (автора) электронного документа от факта отправки (подписи) соответствующего документа или сообщения. Неотрекаемость предполагает, что электронный документ является достоверным, он направлен и подтвержден владельцем регистрационного свидетельства (установлено авторство), содержание электронного документа не имеет несанкционированных изменений после его подтверждения отправителем, автор электронного документа, подтвердивший электронный документ, согласен с содержанием подтвержденного им электронного документа;

15) Носитель ключевой информации – специализированный носитель, в котором для защиты хранящихся закрытых ключей электронной цифровой подписи используется средства криптографической защиты информации, имеющее сертификат соответствия требованиям стандарта СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования»;

16) Облачная ЭЦП – сервис УЦ, 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;

17) Облегченный протокол доступа к каталогам (Lightweight Directory Access Protocol) (далее - LDAP) – протокол прикладного уровня для доступа к службе каталогов, разработанной на рекомендациях стандарта сектора стандартизации электросвязи Международного союза электросвязи (Internation Telecommunication Union - Telecommunication sector) (далее - ITU-T) X.500;

18) Онлайн протокол статуса регистрационного свидетельства (Online Certificate Status Protocol) (далее - OCSP) - протокол для определения статуса регистрационного свидетельства;

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

20) Регистрационное свидетельство – электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным законодательством Республики Казахстан;

21) Работник УЦ – работник Департамента информационной безопасности, отвечающий за администрирование ПО УЦ, HSM УЦ, платформы, обеспечивающей функционирование ПО УЦ;

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

23) Средства криптографической защиты информации (СКЗИ) – совокупность программно-технических средств, реализующих алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами и обеспечивающих применение электронной цифровой подписи и шифрования в информационных системах. Средства криптографической защиты информации могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение;

24) Средства электронной цифровой подписи - совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи;

25) Удостоверяющий центр (далее - УЦ) – АО «Фридом Банк Казахстан», удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, подтверждающее достоверность регистрационного свидетельства;

26) Участник УЦ – Владелец, клиент Банка;

27) Хранилище регистрационных свидетельств – общедоступный реестр всех регистрационных свидетельств;

28) Хэш – преобразование массива входных данных произвольной длины в битовую сторону фиксированной длины;

29) ЦОД – помещение, предназначенное для размещения серверного, активного и пассивного сетевого (телекоммуникационного) оборудования и оборудования структурированных кабельных систем;

30) Электронная цифровая подпись (далее - ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

31) Электронный документ – документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи.

ГЛАВА 2. НАЗНАЧЕНИЯ И ТИПЫ ИМЕН

РАЗДЕЛ 1. НАЗНАЧЕНИЕ ИМЕН

8. Имя регистрационного свидетельства (Distinguished Names (далее – DN)) поля «Subject» идентифицирует участника УЦ, который является Владельцем регистрационного свидетельства и соответствующего закрытого ключа.

Типы имен (наименований)

9. УЦ выдает регистрационные свидетельства, соответствующие рекомендациям ITU-T X.509 версии 3 и RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile). Выданные регистрационные свидетельства содержат в полях «Subject» и «Issuer» сведения, представленные в соответствии с рекомендациями ITU-T X.501 (DN).

Необходимость персональных данных

10. УЦ выдаёт регистрационные свидетельства, которые содержат персональные данные в DN-имени, поля «Subject», позволяющие идентифицировать Владельца регистрационного свидетельства и область применения его регистрационного свидетельства.

Анонимность или использование псевдонимов

11. Анонимность и использование псевдонимов при формировании DN имен не допускается.

Правила интерпретации различных форм имен (наименований)

12. Отличительные DN-имена должны включать все элементы, указанные в соответствующем профиле регистрационного свидетельства, согласно спецификации стандарта X.509 из серии рекомендуемых стандартов ITU-T X.500 и RFC-5280. УЦ заполняет поле «Subject» информацией о Владельце (ФИО, ИИН Заявителя, дополнительно БИН в случае Юридического лица), полученной из государственных баз данных «Физические лица», «Юридические лица», на основании предоставленного Заявителем ИИН и (или) БИН.

Уникальность имен (наименований)

13. Каждому Заявителю УЦ должно соответствовать уникальное DN имя.

РАЗДЕЛ 2. ПРОЦЕДУРА ПЕРВИЧНОЙ РЕГИСТРАЦИИ

14. Первичная регистрация Заявителя – это процесс, в результате которого Заявитель впервые сообщает о себе УЦ, до того, как будет выпущен закрытый ключ ЭЦП для данного Заявителя. Конечным результатом данного процесса (если он успешен) является создание закрытого ключа ЭЦП, выпуск регистрационного свидетельства и помещение его в Хранилище регистрационных свидетельств.

Идентификация при выпуске закрытого ключа ЭЦП в Облачной ЭЦП (физическое лицо)

15. Подача заявлений на создание закрытого ключа ЭЦП в Облачной ЭЦП для физических лиц осуществляется через мобильное приложение Банка.

16. Перед созданием закрытого ключа ЭЦП и выпуском регистрационного свидетельства Заявитель дает согласие на сбор и обработку персональных данных.

17. Для создания закрытого ключа ЭЦП и выпуска регистрационного свидетельства Заявитель должен:

1) пройти процедуру многофакторной аутентификации, одним из методов которой является биометрическая аутентификация;

2) дать согласие на хранение закрытого ключа ЭЦП в HSM Облачной ЭЦП.

18. После создания, закрытый ключ ЭЦП сохраняется в HSM. В качестве секретных значений используется пароль, который в УЦ не хранится.

Идентификация при выпуске закрытого ключа ЭЦП в Облачной ЭЦП для юридических лиц

19. Подача заявлений на создание закрытого ключа ЭЦП в облачной ЭЦП для юридических лиц осуществляется через систему интернет-банкинга Банка для юридических лиц.

20. Перед созданием закрытого ключа ЭЦП и выпуском регистрационного свидетельства Заявитель дает согласие на сбор и обработку персональных данных.

21. В процессе запроса закрытого ключа ЭЦП в облачной ЭЦП Заявитель должен:

1) пройти процедуру многофакторной аутентификации, одним из методов которой является биометрическая аутентификация;

2) дать согласие на хранение закрытого ключа ЭЦП в HSM Облачной ЭЦП.

22. После создания, закрытый ключ облачной ЭЦП сохраняется в HSM. В качестве секретных значений используется пароль, который в УЦ не хранится.

ГЛАВА 3. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА

РАЗДЕЛ 1. ИЗГОТОВЛЕНИЕ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА

Действия УЦ при изготовлении регистрационного свидетельства

23. УЦ изготавливает регистрационное свидетельство в соответствии со сведениями, указанными при регистрации Заявителя. Формат регистрационного свидетельства основан на рекомендациях ITU-T X.509v3 и RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile).

Уведомление заявителя о факте изготовления регистрационного свидетельства

24. Владельцу поступает уведомление об изготовлении регистрационного свидетельства по завершению процесса выпуска регистрационного свидетельства, которое публикуется в Хранилище регистрационных свидетельств.

25. Подписанные Заявление на выдачу регистрационных свидетельств (Приложение №1 к Регламенту), а также Заявление на отзыв регистрационных свидетельств (Приложение №2 к Регламенту), хранятся в базе данных информационной системы, использующей сервисы УЦ.

26. Срок хранения Заявлений определены на постоянной основе в соответствии с Перечнем типовых документов, образующихся в деятельности государственных и негосударственных организаций, с указанием срока хранения.

РАЗДЕЛ 2. ПРИЗНАНИЕ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА

Действия владельца регистрационного свидетельства, означающие признание регистрационного свидетельства

27. Следующие действия Владельца регистрационного свидетельства означают признание регистрационного свидетельства:

1) получение регистрационного свидетельства и/или использование регистрационного свидетельства;

2) отсутствие у Владельца мотивированных возражений (претензий) по поводу содержания регистрационного свидетельства.

Действия владельца регистрационного свидетельства, означающие непризнание регистрационного свидетельства

28. Следующие действия Владельца регистрационного свидетельства означают его непризнание регистрационного свидетельства:

1) Наличие мотивированных возражений (претензий) по содержанию регистрационного свидетельства;

2) Отказ от получения регистрационного свидетельства;

3) Обращение с требованием отзыва регистрационного свидетельства;

4) Явное заявление о непризнании регистрационного свидетельства.

29. В случае, если Владелец регистрационного свидетельства обнаруживает несоответствия, ошибки или неточности в регистрационном свидетельстве, он должен направить мотивированные возражения в письменной форме в адрес УЦ в течение 10 календарных дней с момента получения регистрационного свидетельства.

30. Возражения должны включать описание несоответствий, а также, при необходимости, предложения по их устранению.

31. Если Владелец регистрационного свидетельства отказывается от получения регистрационного свидетельства, он обязан сообщить об этом УЦ в письменной форме до момента получения регистрационного свидетельства или сразу после получения уведомления о его готовности.

32. Отказ от получения регистрационного свидетельства будет расцениваться как непризнание его действительности и отзыва выданного регистрационного свидетельства.

33. В случае, если Владелец регистрационного свидетельства направляет УЦ требование об отзыве регистрационного свидетельства по причине обнаруженных несоответствий или ошибок, регистрационное свидетельство будет считаться непризнанным с момента поступления соответствующего требования.

34. Владелец регистрационного свидетельства может направить в УЦ письменное заявление о непризнании регистрационного свидетельства по любой причине, включая личные соображения или изменившиеся обстоятельства.

35. Регистрационное свидетельство будет считаться непризнанным с момента получения такого заявления УЦ.

Публикация регистрационного свидетельства

36. УЦ публикует регистрационное свидетельство в Хранилище регистрационных свидетельств.

37. Основным протоколом работы хранилища является облегченный протокол доступа к каталогам LDAP. Данный протокол позволяет доверяющим сторонам и участникам УЦ формировать онлайновые запросы, касающиеся информации о статусе регистрационных свидетельств или его изменения, вместе с тем, доступ к информации в хранилище возможен через web-интерфейс.

38. УЦ предоставляет информацию о том, по каким адресам находятся соответствующее хранилище и служба онлайнового протокола статуса регистрационных свидетельств (OCSP).

39. УЦ публикует регистрационные свидетельства, которые он выпустил. В случае отзыва регистрационного свидетельства УЦ удаляет это регистрационное свидетельство из хранилища.

39-1. Протоколы событий ежедневно преобразуется в хэш, и данные хэш хранятся в цепочке событий блокчейн. Мониторинг системы блокчейн доступен в сети Интернет по ссылке:https://my.bankffin.kz/digital-signature/blockchain/?limit=100&offset=0.

Уведомление участника УЦ о выдаче регистрационного свидетельства

40. Официальным уведомлением пользователей УЦ о выдаче регистрационного свидетельства является его публикация в Хранилище регистрационных свидетельств и уведомление в приложениях Банка.

РАЗДЕЛ 3. ИСПОЛЬЗОВАНИЕ КЛЮЧЕЙ И РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА

41. Закрытый ключ ЭЦП используется для формирования электронной цифровой подписи с использованием средств электронной цифровой подписи.

42. Регистрационное свидетельство используется для подтверждения соответствия ЭЦП. Проверка производится в соответствии с Правилами Проверки подлинности электронной цифровой подписи, утвержденными приказом Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187.

Использование закрытого ключа ЭЦП и регистрационного свидетельства их владельцем

43. Использование регистрационного свидетельства не должно противоречить действующему законодательству Республики Казахстана в сфере ЭЦП, а также настоящему Регламенту.

44. При использовании закрытых ключей ЭЦП, хранящихся в УЦ, владелец проходит многофакторную аутентификацию, одним из методов является биометрическая аутентификация.

45. Подписание электронных документов осуществляется в памяти HSM путем передачи подписываемого файла или его хэш в HSM.

46. При аутентификации владельца в УЦ передача пароля от владельца (браузер, мобильное приложение) в HSM производится в зашифрованном виде~~, при этом шифрование пароля производится на стороне владельца, в персональном компьютере или смартфоне.~~

47. Восстановление пароля от закрытого ключа ЭЦП в облачной ЭЦП не осуществляется.

Использование открытого ключа и регистрационного свидетельства пользователем

48. Владелец регистрационного свидетельства должен использовать регистрационного свидетельства строго в соответствии с указанными в нем сведениями и настоящим Регламентом.

РАЗДЕЛ 4. ЗАМЕНА/ПЕРЕВЫПУСК КЛЮЧЕЙ

49. Замена/перевыпуск закрытого ключа ЭЦП – процедура изготовления нового закрытого ключа ЭЦП и соответствующего ему регистрационного свидетельства.

Основания для замены/перевыпуска закрытого ключа ЭЦП

50. Закрытые ключи ЭЦП могут быть заменены, если до истечения срока действия регистрационного свидетельства осталось менее чем 30 календарных дней (один месяц), а также при подозрении на компрометацию закрытого ключа ЭЦП.

51. При подозрении на компрометацию закрытого ключа ЭЦП Владелец регистрационного свидетельства обязан незамедлительно направить запрос на отзыв регистрационного свидетельства через мобильные приложения и/или сайты Банка.

52. В случае замены закрытого ключа ЭЦП до истечения срока действия текущего регистрационного свидетельства пользователь самостоятельно принимает решение о необходимости его отзыва.

РАЗДЕЛ 5. ИЗМЕНЕНИЕ СВЕДЕНИЙ, УКАЗАННЫХ В РЕГИСТРАЦИОННОМ СВИДЕТЕЛЬСТВЕ

53. Изменение сведений, указанных в регистрационном свидетельстве, не допускается.

РАЗДЕЛ 6. ОТЗЫВ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА

Основания для отзыва регистрационного свидетельства

54. УЦ отзывает регистрационное свидетельство и осуществляет публикацию его в СОРС в соответствии со статьей 18 Закона Республики Казахстан от 7 января 2003 года «Об электронном документе и электронной цифровой подписи» в следующих случаях:

1) по требованию Владельца регистрационного свидетельства либо его представителя;

2) при установлении 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) смены наименования, реорганизации, ликвидации юридического лица – владельца регистрационного свидетельства, смены руководителя юридического лица;

6) предусмотренных соглашением между УЦ и Владельцем регистрационного свидетельства;

7) по вступившему в законную силу решению суда.

Лица, уполномоченные подавать заявления на отзыв регистрационного свидетельства

55. Заявление на отзыв регистрационного свидетельства физического лица может подавать его Владелец. В случае юридического лица доступ к системе интернет-банкинга может быть заблокирован по инициативе Банка при сверке данных юридического лица с государственными сервисами и базами данных Республики Казахстан на предмет обнаружения несоответствий – реорганизация, ликвидация, смена данных юридического лица. Юридическое лицо вправе обратиться в отделения Банка для актуализации своих данных.

Процедура идентификации и аутентификации заявления

56. Процедура идентификации Владельца регистрационного свидетельства при обработке Заявления на отзыв, подписанного закрытым ключом ЭЦП, выполняется на основании данных, указанных в Заявлении на отзыв. Процесс отзыва регистрационного свидетельства возможен через мобильное приложение Банка для физических лиц и систему интернет-банкинга для юридических лиц с применением многофакторной аутентификации.

Срок подачи заявления на отзыв регистрационного свидетельства

57. Заявление на отзыв следует подавать в течение минимально возможного времени после появления такой необходимости (например, в случае подозрения на компрометацию закрытого ключа ЭЦП).

Срок обработки заявления на отзыв регистрационного свидетельства

58. УЦ обрабатывает Заявление на отзыв регистрационного свидетельства незамедлительно, но не более одного рабочего дня, следующего за днем получения УЦ Заявления на отзыв. В случае успешного рассмотрения Заявления на отзыв регистрационное свидетельство публикуется в СОРС.

Частота выпуска списков отозванных регистрационных свидетельств

59. СОРС обновляется по мере отзыва регистрационного свидетельства. Отозванные регистрационные свидетельства с истекшим сроком хранения удаляются из СОРС.

Другие способы извещения участников информационных систем о фактах отзыва регистрационных свидетельств

60. Официальным уведомлением участников УЦ об отзыве регистрационного свидетельства является публикация информации в СОРС и приложении Банка.

Срок хранения отозванных регистрационных свидетельств

61. Срок хранения отозванных регистрационных свидетельств в Хранилище регистрационных свидетельств составляет не менее 5 (пяти) лет.

Особые требования в случае компрометации закрытого ключа ЭЦП

62. В случае компрометации закрытого ключа ЭЦП Владелец соответствующего регистрационного свидетельства обязан в кратчайшие сроки любыми доступными способами обратиться в УЦ с установленной формой Заявления на отзыв, а УЦ по получении такого заявления должен немедленно отозвать регистрационное свидетельство.

РАЗДЕЛ 7. СЕРВИС ПРОВЕРКИ СТАТУСА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА В РЕЖИМЕ ONLINE

Эксплуатационные характеристики

63. Информация о статусах регистрационных свидетельств доступна с использованием СОРС и сервиса OCSP, публикуемого по адресу: https://pki.bankffin.kz/cgi/RevList.crl.

64. СОРС предоставляется в электронной форме в формате, определенном RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile). СОРС заверяется корневым регистрационным свидетельством УЦ. Доступ к СОРС обеспечивается по протоколам LDAP (RFC 2251 Lightweight Directory Access Protocol (v3)) и HTTP.

65. Сервис OCSP соответствует требованиям, описанным в RFC 2560 (Online Certificate Status Protocol). Квитанции с результатом проверки регистрационного свидетельства в режиме online заверяются ЭЦП сервера OCSP.

Доступность службы проверки статусов регистрационных свидетельств

66. Информация о статусах регистрационных свидетельств доступна постоянно без запланированных перерывов в работе УЦ.

РАЗДЕЛ 8. ОКОНЧАНИЕ ПОЛЬЗОВАНИЯ УСЛУГАМИ УЦ

67. Регистрационные свидетельства пользователей УЦ становятся недействительными при истечении срока их действия. Участник ИС может закончить использование услуг УЦ путем отзыва регистрационного свидетельства или отказа от смены закрытого ключа ЭЦП после окончания его срока действия.

РАЗДЕЛ 9. ДЕПОНИРОВАНИЕ И ВОССТАНОВЛЕНИЕ КЛЮЧЕЙ

68. УЦ не допускает депонирование и восстановление закрытых ключей ЭЦП Владельцев регистрационных свидетельств.

ГЛАВА 4. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

РАЗДЕЛ 1. ФИЗИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Размещение УЦ

69. УЦ, обрабатывающий запросы участников УЦ, расположен в ЦОД, которое соответствует необходимым требованиям Правил организации центров обработки данных в АО «Фридом Банк Казахстан».

Физический доступ в помещения ЦОД

70. Помещения ЦОД УЦ оборудованы системой контроля и управления доступом с идентификацией по смарт-картам, исполнительными устройствами системы контроля доступа электромеханического типа, включая систему видеонаблюдения.

Электроснабжение и кондиционирование воздуха

71. Технические средства УЦ подключены к гарантированной сети электроснабжения Банка. Электрические сети и электрооборудование, используемые в серверном помещении, отвечают требованиям Правил организации центров обработки данных в АО «Фридом Банк Казахстан».

72. Серверы и телекоммуникационное оборудование УЦ подключены к источникам бесперебойного питания. ЦОД оборудовано средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Подверженность воздействию влаги

73. Защита оборудования УЦ от влаги обеспечивается его размещением в специальных серверных шкафах.

Противопожарные меры безопасности и защита от возгорания

74. Помещения ЦОД УЦ оборудованы средствами пожаротушения в соответствии с требованиями, установленными законодательством РК.

Хранение архивных документов и электронных носителей

75. Электронный архив УЦ хранится в соответствии с действующим законодательством Республики Казахстан.

Уничтожение документированной информации

76. Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется уполномоченными лицами УЦ, обеспечивающими документирование.

Сменные носители информации физически уничтожаются перед утилизацией в соответствии с Правилами использования мобильных устройств и носителей информации АО «Фридом Банк Казахстан».

РАЗДЕЛ 2. ОРГАНИЗАЦИОННЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Разграничение ролей (полномочий)

77. Роли работников УЦ:

1) Администратор УЦ (администрирование ПО УЦ, администрирование HSM УЦ);

2) Системный администратор УЦ (администрирование платформы для функционирования ПО УЦ).

РАЗДЕЛ 3. ТРЕБОВАНИЯ К ПЕРСОНАЛУ УЦ

Требования к квалификации и стажу работы

78. Требования к квалификации и стажу Работников УЦ определяются должностными инструкциями соответствующего подразделения Банка.

Процедура проверки биографии работника

79. Проверка биографии работников УЦ осуществляется в соответствии с внутренними инструкциями Департамента безопасности Банка.

Требования к повышению квалификации персонала

80. Вновь принятые работники УЦ обязаны пройти обучение основам информационной безопасности, проводимое ДИБ.

В случае значительных изменений в программном либо аппаратном обеспечении УЦ Производитель ПО УЦ и HSM проводит обучение работников УЦ по использованию обновленных компонентов.

Требования к независимым подрядчикам

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

Документация, предоставляемая персоналу

82. Деятельность работников УЦ регламентирована внутренними нормативно-техническими документами УЦ.

83. Доступ работников УЦ к документам и документации, составляющей документальный фонд УЦ, организован в соответствии с должностными инструкциями и функциональными обязанностями.

РАЗДЕЛ 4. ПОРЯДОК ВЕДЕНИЯ ЗАПИСЕЙ АУДИТА

Типы событий, подлежащих аудиту

84. Программно-аппаратный комплекс УЦ регистрирует следующие виды событий:

1) системные события общесистемного программного обеспечения;
2) принятие запроса на выпуск/отзыв регистрационного свидетельства;
3) выпуск/отзыв регистрационного свидетельства;
4) помещение запроса на регистрационное свидетельство;
5) принятие запроса на регистрационное свидетельство;
6) отклонение запроса на регистрационное свидетельство;
7) выпуск/перевыпуск CORC;
8) невыполнение внутренней операции программной компоненты.

85. Структуры записей событий соответствуют эксплуатационной документации программного обеспечения, реализации целевых функций УЦ и общесистемному программному обеспечению.

86. Для облачной ЭЦП УЦ обеспечивает регистрацию следующих событий:

1) формирование закрытого ключа ЭЦП облачной ЭЦП;
2) использование закрытого ключа ЭЦП облачной ЭЦП;
3) удаление (стирание) закрытого ключа ЭЦП облачной ЭЦП.

87. Срок хранения протоколов работы составляет 1 (один) год с даты истечения срока хранения регистрационного свидетельства.

88. При регистрации действий пользователей записывается следующая информация:

1) идентификатор Владельца;
2) дата, время;
3) событие.

Частота анализа журналов аудита

89. Журналы аудита еженедельно анализируются работниками УЦ с целью обнаружения нарушений в работе программного и аппаратного обеспечения УЦ, анализа производительности систем.

В процессе анализа журналов аудита проводится разбор всех значительных сбоев в работе, и принимаются соответствующие меры реагирования, которые впоследствии находят отражение в новых версиях ПО.

Результаты анализа значительных сбоев в работе УЦ, оказавшие прямое или косвенное влияние на результативность работы бизнес-процессов УЦ или их остановку/аварию, доводятся работниками УЦ до Департамента информационной безопасности (далее – ДИБ) и Департамента операционных, ИТ/ИБ рисков и внутреннего контроля Банка для дальнейшего анализа и принятия решений.

Срок хранения журналов аудита

90. Журналы аудита подлежат архивированию по истечении 2 (двух) месяцев после окончания их анализа.

Защита журналов аудита

91. Журналы аудита защищены от несанкционированного просмотра, модификации и удаления средствами прикладного и общесистемного программного обеспечения.

Резервное копирование журналов аудита

92. Журналы аудита подлежат резервному копированию ежедневно.

Анализ уязвимостей

93. Записи в журнале аудита анализируются работниками ДИБ с целью выявления аномалий и потенциальных угроз. ДИБ на постоянной основе выполняют мониторинг уязвимостей УЦ в соответствии с ВНД Банка.

РАЗДЕЛ 5. ВЕДЕНИЕ АРХИВА

Срок хранения архива

94. Архивированию подлежит следующие документированные материалы:

1) досье Заявителя, включающее копии документов, предоставленных Заявителем при подаче Заявления;

2) Заявления на выдачу и отзыв (аннулирование);

3) копия регистрационного свидетельства;

4) соглашения с Владельцами регистрационных свидетельств, договоры (при наличии);

5) акты уничтожения закрытых ключей облачной ЭЦП и другие связанные документы.

Архивное хранение данной информации осуществляется как в электронной форме в соответствующих системах, так и на бумажных носителях, в соответствии с законодательством Республики Казахстан и внутренними нормативными документам Банка.

Срок хранения указанных документов -определены на постоянной основе согласно Перечню типовых документов, образующихся в деятельности государственных и негосударственных организаций, с указанием срока хранения (далее - Перечень).

Резервное копирование архива

95. Электронные носители архива подлежат резервному копированию ежедневно.

Порядок получения и проверки информации, хранящейся в архиве

96. Доступ к электронному архиву имеют только работники УЦ.

РАЗДЕЛ 6. СМЕНА КЛЮЧЕЙ УЦ

97. Заблаговременно до окончания срока действия закрытых ключей ЭЦП УЦ работник УЦ производит формирование новых закрытых ключей и регистрационных свидетельств УЦ и публикует их в соответствующем разделе Хранилища регистрационных свидетельств.

98. Ответственность за смену закрытых ключей УЦ возлагается на администратора УЦ.

РАЗДЕЛ 7. ВОССТАНОВЛЕНИЕ В СЛУЧАЕ КОМПРОМЕТАЦИИ ИЛИ СБОЕВ

Действия по предотвращению компрометации и сбоев

99. Данные УЦ подлежат обязательному архивированию и резервному копированию для предотвращения потери данных. Резервное копирование Хранилища регистрационных свидетельств и СОРС осуществляется не реже одного раза в сутки. Архивирование данных УЦ выполняется в соответствии с ВНД по архивированию информации в Банке.

Действия по предотвращению повреждения оборудования, программных и/или аппаратных сбоев

100. В случае повреждения оборудования, программных или аппаратных сбоев информация о происшествии, зафиксированная работниками ДИБ, подлежит тщательному расследованию. После завершения всех мероприятий по расследованию и устранению последствий инцидента результаты и информация направляются директору ДИБ и в Департамент операционных, ИТ/ИБ рисков и внутреннего контроля через корпоративную электронную почту. Директор ДИБ осуществляет контроль за выполнением работниками необходимых мероприятий по устранению последствий и предотвращению повторения подобных инцидентов в дальнейшем. Департамент операционных, ИТ/ИБ рисков и внутреннего контроля выполняет анализ полученной информации о происшествии с целью

выявления потенциальных рисков и уязвимостей, которые могли привести к инциденту. Восстановительные работы выполняются в соответствии с внутренним планом аварийного восстановления.

РАЗДЕЛ 8. РАЗРЕШЕНИЕ КОНФЛИКТНЫХ СИТУАЦИЙ

Непризнание отправителем/получателем электронного документа его целостности и подлинности

101.Разбор конфликтной ситуации осуществляется в соответствии с Главой 9 настоящего Регламента.

Процедура проверки ЭЦП электронного документа

102.Процедура проверки ЭЦП электронного документа выполняется автоматически в ИС в соответствии с Правилами проверки подлинности электронной цифровой подписи (приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 г. № 1187).

РАЗДЕЛ 9. ПРЕКРАЩЕНИЕ РАБОТЫ УЦ

103. Деятельность УЦ прекращается в порядке, установленном законодательством РК.В случае прекращения деятельности УЦ Работник УЦ обязан уведомить всех участников, обслуживаемых им информационных систем, а также Министерство искусственного интеллекта и цифрового развития Республики Казахстан, не позднее чем за 30 (тридцать) дней до прекращения своей деятельности .

104.При прекращении деятельности УЦ, выданные им регистрационные свидетельства и соответствующие закрытые ключи ЭЦП, сведения о Владельцах регистрационных свидетельств передаются в другие удостоверяющие центры Работником УЦ по согласованию с Владельцем регистрационного свидетельства.

105.По истечении срока в 30 (тридцать) дней регистрационное свидетельство и соответствующие ключи электронной цифровой подписи, не переданные в другие удостоверяющие центры, прекращают свое действие и подлежат хранению в соответствии с законодательством РК.

ГЛАВА 5. ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

РАЗДЕЛ 1. ИЗГОТОВЛЕНИЕ И УСТАНОВКА КЛЮЧЕВОЙ ПАРЫ

Изготовление ключей и используемые алгоритмы

106.Закрытые ключи ЭЦП создаются в облачной ЭЦП. Закрытые ключи ЭЦП облачной ЭЦП генерируются строго внутри HSM (в сертифицированных криптографических модулях Certex HSM II, Certex HSM ES III.) Закрытый ключ не извлекается из HSM в открытом виде. УЦ обеспечивает защиту закрытых ключей ЭЦП в УЦ.

107.При этом HSM:

1) соответствует не ниже третьему уровню 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 Республики Казахстан.

После создания закрытый ключ ЭЦП сохраняется в HSM в зашифрованном виде с использованием стандарта ГОСТ 28147-89. В качестве секретных значений участвуют пароль, заданный Владельцем, который в УЦ не хранится. УЦ для проверки пароля от закрытого ключа владельца хранит хэш пароля в HSM.

Передача открытых ключей подписей УЦ участникам информационных систем

108. Предоставление открытого ключа реализовано посредством публикации его регистрационного свидетельства в Хранилище регистрационных свидетельств и на веб-сайте: https://bankffin.kz.

До начала использования регистрационного свидетельства Владелец должен получить открытый ключ.

Получив регистрационное свидетельство, Владелец подтверждает свое полное и безоговорочное согласие с условиями использования сервисов УЦ.

Размеры ключей

109. При использовании криптографического преобразования по алгоритму ГОСТ 34.310-2004:

1) закрытый ключ – 256 бит;
2) открытый ключ – 512 бит.

Цели использования ключа (порядок заполнения поля key usage сертификата x.509v3)

110. Заполняются в соответствии с политикой регистрационного свидетельства.

РАЗДЕЛ 2. ЗАЩИТА ЗАКРЫТОГО КЛЮЧА, ТРЕБОВАНИЯ К КРИПТОГРАФИЧЕСКИМ МОДУЛЯМ

Контроль закрытого ключа (n из m), контролируемый несколькими держателями

111. В соответствии с эксплуатационной документацией средства криптографической защиты информации.

Резервное копирование закрытого ключа

112. Архивирование ключевой информации с HSM возможно только в зашифрованном виде и только с разделением ключа шифрования по схеме M из N (не менее 3 из 5). Ключи шифрования по схеме M из N хранятся на защищенных токенах. Защищенные токены используются только при восстановлении архива на резервном HSM.

Архивирование закрытого ключа

113. Закрытые ключи с истекшим сроком действия подлежат уничтожению в соответствии с эксплуатационной (технической) документацией средства криптографической защиты информации. Архивное хранение закрытых ключей не допускается.

Способы уничтожения закрытого ключа

114. Уничтожение закрытого ключа производится в соответствии с эксплуатационной документацией средства криптографической защиты информации.

Хранение закрытого ключа УЦ в HSM и закрытых ключей Владельцев

115. HSM, хранящие закрытые ключи УЦ, аппаратно не допускают хранения ключевого материала в незашифрованном виде, в том числе в оперативной памяти устройства.

116. Закрытые ключи владельцев, хранящиеся в HSM, хранятся в соответствии с требованиями стандарта PKCS#11.

РАЗДЕЛ 3. ДРУГИЕ ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ КЛЮЧЕЙ

Архивирование открытых ключей подписей

117. Все регистрационные свидетельства архивируются в соответствии с порядком резервного копирования, установленным в Банке.

Сроки действия регистрационных свидетельств и ключей

118. Начало периода действия регистрационного свидетельства Центра Сертификации исчисляется с даты и времени его генерации. Срок действия корневого регистрационного свидетельства УЦ составляет 20 (двадцать) лет. Срок действия регистрационного свидетельства УЦ составляет 10 (десять) лет.

119. Срок действия регистрационного свидетельства Владельца составляет 1 (один) год. Начало периода действия закрытого ключа Владельца регистрационного свидетельства исчисляется с даты и времени начала действия соответствующего регистрационного свидетельства Владельца.

Ограничения на использования ключей

120. Закрытый ключ Центра Сертификации используется для формирования ЭЦП регистрационных свидетельств Владельцев и СОРС.

Закрытые ключи ЭЦП Владельцев используются для формирования ЭЦП электронных документов и авторизации в информационных/финансовых системах.

РАЗДЕЛ 5. СРЕДСТВА УПРАВЛЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТЬЮ

121. Компьютеры, работающие в УЦ, должны удовлетворять требованиям политики информационной безопасности, утвержденной Банком.

РАЗДЕЛ 6. СПИСАНИЕ ОБОРУДОВАНИЯ

122. Списание оборудования происходит согласно внутренним нормативным документам Банка.

ГЛАВА 6. ПРОВЕРКА СООТВЕТСТВИЯ И ДРУГИЕ ОЦЕНКИ

РАЗДЕЛ 1. ТЕМЫ, ЗАТРАГИВАЕМЫЕ ПРИ ПРОВЕДЕНИИ ОЦЕНКИ

123. В рамках аккредитации УЦ рассматривается полнота и качество выполнения корпоративных требований в отношении хозяйственной деятельности и программно-технического комплекса, в том числе:

1) целостность услуг;
2) управление информационной безопасностью;
3) управление доступом;
4) протоколирование;
5) распространение публичных ключей УЦ;
6) архивирование ключей УЦ;
7) выдача регистрационных свидетельств УЦ;

8) отзыв регистрационных свидетельств УЦ.

РАЗДЕЛ 2. ДЕЙСТВИЯ, ПРЕДПРИНИМАЕМЫЕ В РЕЗУЛЬТАТЕ НЕСООТВЕТСТВИЯ ФУНКЦИОНИРОВАНИЯ УЦ ДАННОМУ ДОКУМЕНТУ И СООБЩЕНИЯ О РЕЗУЛЬТАТАХ

124. При выявлении нарушений в функционировании УЦ действия пользователей УЦ, работников УЦ регулируются внутренним нормативным документом реагирования на инциденты информационной безопасности.

ГЛАВА 7. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

РАЗДЕЛ 1. ПРЕДЕЛЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

125. УЦ признаёт, что информация, доступ к которой ограничивается в соответствии с законодательством РК и внутренними нормативными документами Банка, рассматривается в качестве конфиденциальной информации.

126. OTP-пароль является конфиденциальной информацией.

Информация не являющаяся конфиденциальной

127. Участники УЦ признают, что содержимое регистрационных свидетельств, информация об их отзыве, о статусе регистрационных свидетельств, публичная часть Хранилища регистрационных свидетельств и содержащаяся в нем информация не является конфиденциальной информацией.

Обязательства по защите конфиденциальной информации

128. Участники УЦ обязуется:

1) не разглашать конфиденциальную информацию и использовать ее только в целях, для которых она была передана (получена);

2) соблюдать и принимать установленные УЦ меры по охране конфиденциальной информации:

- хранение и использование конфиденциальной информации должно осуществляться УЦ в местах, обеспечивающих физическую сохранность конфиденциальной информации и авторизацию доступа;
- на устройствах, являющихся материальным носителем ключевой информации, должны быть установлены пароли, с целью обеспечить сохранность данной информации и исключить доступ к конфиденциальной информации всех лиц, кроме лица, уполномоченного владеть доступом к носителю;
- любая попытка извлечения конфиденциальной информации за пределы мест ее хранения/использования не допускается;
- исключить возможность ознакомления с конфиденциальной информацией лиц, не уполномоченных на такое ознакомление (доступ);
- при утере (повреждении) или разглашении, подозрении либо угрозе разглашения (компрометации) конфиденциальной информации, а также при обнаружении признаков незаконного получения (использования) конфиденциальной информации третьими лицами, незамедлительно сообщить об этом УЦ, обратившись в Банк с Заявлением на отзыв регистрационного свидетельства.

Разглашение информации в случаях, установленных законодательством

129. Деятельность УЦ регулируется законодательством РК. УЦ обязуется использовать конфиденциальную и личную информацию в соответствии с установленным в Регламенте порядком.

ГЛАВА 8. ОБЯЗАННОСТИ

РАЗДЕЛ 1. ОБЯЗАННОСТИ УЦ

130. УЦ ответственен за создание закрытых ключей ЭЦП и соответствующих им регистрационных свидетельств, последующее управление ими в соответствии с настоящим Регламентом, в частности, он:

1) обрабатывает запросы на создание закрытых ключей ЭЦП регистрационных свидетельств и выдачу регистрационных свидетельств для Владельцев в соответствии с запрашиваемой областью применения (политикой);
2) предоставляет сведения о статусе выпущенных регистрационных свидетельств по запросам заявителей при обращении в УЦ;
3) обеспечивает доступ к Хранилищу регистрационных свидетельств;
4) публикует информацию о выпущенных регистрационных свидетельствах в Хранилище регистрационных свидетельств;
5) публикует корневое регистрационное свидетельство УЦ в Хранилище регистрационных свидетельств;
6) подтверждает запросы на отзыв регистрационных свидетельств;
7) выпускает CORC;
8) публикует информацию об отозванных регистрационных свидетельствах.

131. УЦ обеспечивает отсутствие возможности подписания электронных документов с использованием закрытых ключей ЭЦП Облачной ЭЦП без ведома (аутентификации) Владельца.

РАЗДЕЛ 2. ПРАВА И ОБЯЗАННОСТИ ВЛАДЕЛЬЦА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА

132. Предоставляя в УЦ Заявление, Заявители соглашаются:

1) принять условия и следовать процедурам, описанным в настоящем Регламенте;
2) предоставить достоверную и точную информацию при регистрации в УЦ;
3) своевременно уведомлять УЦ об изменении своих учетных данных, предоставленных в документах при регистрации;
4) использовать сервисы УЦ в соответствии с настоящим Регламентом;
5) применять для формирования ЭЦП только действующий закрытый ключ ЭЦП, соответствующий открытому ключу ЭЦП, указанному в регистрационном свидетельстве Владельца;
6) применять закрытые ключи и соответствующие им регистрационные свидетельства в соответствии с областью применения и политиками, указанными в регистрационном свидетельстве.

РАЗДЕЛ 3. ОБЯЗАННОСТИ ДОВЕРЯЮЩИХ СТОРОН

133. При использовании регистрационного свидетельства, выданного УЦ, доверяющие стороны соглашаются:

1) принять условия и следовать процедурам, описанным в настоящем Регламенте;
2) проверить срок действия и политику регистрационного свидетельства;
3) проверить статус регистрационного свидетельства, используя CORC и/или OSCP;

4) использовать регистрационное свидетельство в соответствии с настоящим Регламентом, политикой применения регистрационного свидетельства и действующим законодательством.

РАЗДЕЛ 4. ОТЗЫВ ГАРАНТИЙ

134. УЦ не несет ответственности за последствия, возникшие в результате нарушения Владельцами, участниками ИС и/или доверяющими сторонами положений настоящего Регламента и/или действующего законодательства.

РАЗДЕЛ 5. ОГРАНИЧЕНИЯ ОТВЕТСТВЕННОСТИ

135. УЦ гарантирует обработку запросов на выдачу регистрационного свидетельства согласно процедурам, описанным в настоящем Регламенте.

УЦ гарантирует обработку запросов на отзыв регистрационного свидетельства согласно процедурам, описанным в настоящем Регламенте.

УЦ гарантирует отсутствие в регистрационных свидетельствах умышленного искажения данных их Владельцев.

Претензии к УЦ ограничиваются указанием на несоответствие его действий настоящему Регламенту.

ГЛАВА 9. ДРУГИЕ ЮРИДИЧЕСКИЕ ВОПРОСЫ

РАЗДЕЛ 1. СРОК ДЕЙСТВИЯ И ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ РЕГЛАМЕНТА УЦ

Срок действия

136. Регламент вступает в силу с момента его публикации на сайте Банка и действует до публикации новой редакции Регламента. Изменения, внесенные в Регламент, вступают в силу с момента его публикации на сайте Банка в новой редакции.

Внесение изменений/прекращение действия Регламента УЦ

137. В случае внесения изменений либо прекращения действия Регламента УЦ все действующие регистрационные свидетельства остаются связанными с Регламентом и действуют до момента истечения срока действия регистрационного свидетельства.

Участников УЦ не уведомляют заранее о внесении изменений в настоящий Регламент. Изменения утверждают прежде, чем новый документ будет опубликован.

138. УЦ вправе прекратить действие Регламента в одностороннем порядке с соблюдением требований законодательства Республики Казахстан и внутренних нормативных документов Банка.

Основания, при которых номер версии документа должен быть изменен

139. Номер версии документа обновляется всякий раз, когда в документ вносятся изменения.

РАЗДЕЛ 2. ПОРЯДОК ПРОВЕДЕНИЯ ЭКСПЕРТИЗЫ ПРИ ВОЗНИКНОВЕНИИ СПОРНЫХ СИТУАЦИЙ

140. В случаях разногласий УЦ предоставляет Участникам УЦ всю имеющуюся информацию: подтверждает/не подтверждает достоверность регистрационного свидетельства, удостоверяет соответствие открытого ключа Электронной цифровой подписи закрытому ключу Электронной цифровой подписи, а также проводит иные проверки, предусмотренные законодательством Республики Казахстан.

141. В случае возникновения конфликтной ситуации Сторона, предполагающая возникновение конфликтной ситуации, должна в течение 1 рабочего дня после возникновения конфликтной ситуации направить уведомление о возникновении конфликтной ситуации другой Стороне.

142. Уведомление о наличии конфликтной ситуации оформляется и отправляется в виде электронного письма, а в случае, если это невозможно, то составляется на бумажном носителе и направляется с нарочным, либо иным способом, обеспечивающим подтверждение вручения уведомления адресату Уведомление о предполагаемой конфликтной ситуации должно содержать информацию о существе конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации, а также требования к другой Стороне. В уведомлении должны быть указаны фамилия, имя и отчество, должность, контактные телефоны, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.

143. Сторона, которой направлено уведомление, обязана в течение 5 (пяти) рабочих дней проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить уведомителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

После получения информации уведомителем:

1) конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от Стороны, которой было направлено уведомление, и отзывает свои требования, указанные в уведомлении;

2) в случае если уведомитель не удовлетворен информацией, полученной от Стороны, которой направлялось уведомление, для рассмотрения конфликтной ситуации формируется экспертно-техническая комиссия (далее – Комиссия).

В состав Комиссии включаются представители участника ИС, Банка (с привлечением работника УЦ).

144. Сформированная Комиссия при рассмотрении конфликтной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени отправки Электронного документа, его подлинности, а также о подписании Электронного документа конкретной ЭЦП, аутентичности отправленного документа полученному.

Все действия, предпринимаемые Комиссией для выяснения фактических обстоятельств, а также выводы, сделанные Комиссией, заносятся в Протокол работы экспертно-технической комиссии. Данный протокол является основным документом работы Комиссии и должен быть подписан всеми ее членами.

145. По итогам работы Комиссии составляется Акт в необходимом количестве экземпляров (по числу членов комиссии), который подписывается всеми членами Комиссии и направляется каждой из Сторон по одному экземпляру. Акт содержит следующую информацию:

1) фактические обстоятельства, послужившие основанием возникновения разногласий;

2) протокол работы Комиссии;

3) выводы Комиссии.

146. Если на предложение УЦ о создании Комиссии ответ участника ИС не был получен или получен отказ от содействия в работе Комиссии или если участником ИС чинились препятствия в работе Комиссии, УЦ вправе составить акт в одностороннем порядке с указанием причины его составления. В акте приводится обоснование выводов о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого Электронного документа. Указанный акт составляется в двух экземплярах, подписывается УЦ, и один экземпляр направляется участнику ИС по почте.

Стороны признают, что Акт, составленный Комиссией, является обязательным для Сторон и может служить доказательством при дальнейшем разбирательстве спора в суде в случае отсутствия согласия по спорным вопросам.

РАЗДЕЛ 3. ДЕЙСТВУЮЩЕЕ ЗАКОНОДАТЕЛЬСТВО

147. Юридическая сила, толкование данного документа осуществляется в соответствии с действующим законодательством РК.

РАЗДЕЛ 4. СООТВЕТСТВИЕ ДЕЙСТВУЮЩЕМУ ЗАКОНОДАТЕЛЬСТВУ

148. УЦ осуществляет свою деятельность в соответствии с действующим законодательством РК.

РАЗДЕЛ 5. РАЗЛИЧНЫЕ ПОЛОЖЕНИЯ

Независимость разделов документов

149. В случае если часть положений настоящего Регламента будет признана неосуществимой судом, законодательством РК или уполномоченным государственным органом, остальная его часть сохраняет силу.

Форс-мажор

150. УЦ освобождается от ответственности за неисполнение либо ненадлежащее исполнение своих обязательств в соответствии с настоящим Регламентом, если оно явилось следствием наступления обстоятельств непреодолимой силы.

151. Обстоятельства непреодолимой силы включают, но не ограничиваются:

1) Стихийные бедствия (землетрясения, наводнения, ураганы, цунами, пожары и другие природные катастрофы).

2) Военные действия, акты терроризма, гражданские беспорядки, массовые беспорядки.

3) Действия государственных органов или органов местного самоуправления, включая введение чрезвычайного положения, карантина или других ограничительных мер.

4) Забастовки, локауты и другие трудовые конфликты, которые оказывают значительное влияние на возможность выполнения обязательств.

5) Пожары, взрывы, аварии на объектах инфраструктуры Банка, отключения электроэнергии, сбои в работе телекоммуникационных сетей и других инженерных систем, влияющие на функционирование УЦ.

6) Кибератаки и иные действия третьих лиц, направленные на нарушение работы информационных систем УЦ, которые невозможно было предвидеть и предотвратить разумными мерами.

152. В случае наступления обстоятельств непреодолимой силы:

1) УЦ обязуется незамедлительно уведомить участников ИС и Министерство искусственного интеллекта и цифрового развития Республики Казахстан о возникших обстоятельствах.

2) УЦ принимает все возможные меры для минимизации последствий и возобновления исполнения своих обязательств в максимально короткие сроки.

3) Сроки исполнения обязательств УЦ продлеваются на период действия обстоятельств непреодолимой силы и времени, необходимого для устранения их последствий.

РАЗДЕЛ 6. ПРАВА НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ

153. Банк оставляет за собой права интеллектуальной собственности на регистрационные свидетельства, которые выпускает УЦ, и на информацию об их статусе. При этом не запрещается копирование и распространение регистрационных свидетельств на неисключительной безвозмездной основе при соблюдении условий полноты копирования и использования регистрационных свидетельств в соответствии с настоящим Регламентом. УЦ также не запрещает использование информации о статусе регистрационных свидетельств для выполнения функций доверяющей стороны в соответствии с настоящим Регламентом. Владельцы УЦ сохраняют все свои права на все торговые и тому подобные марки и имена, содержащиеся в Заявлениях, и на отличительные (DN) имена в выпущенных регистрационных свидетельствах.

Ключевые пары, которые соответствуют регистрационным свидетельствам, выпущенным УЦ, составляют собственность (в том числе интеллектуальную) Владельцев регистрационных свидетельств в независимости от физических носителей, на которых хранятся эти ключевые пары и которыми они защищаются.

ГЛАВА 10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

154. Внесение изменений и дополнений в Регламент осуществляется в соответствии с требованиями Правил разработки, утверждения, изменения и/или дополнения и прекращения действия внутренних документов Банка, утвержденных Банком.

155. Ответственность за внесение изменений в Регламент несет ДИБ Банка.

156. Пересмотр настоящего Регламента может быть, как плановый, так и внеплановый –обусловленный изменениями в действующем законодательстве или в технологии работы подразделений УЦ, предложениями и замечаниями аудиторов, рекомендациями внешних экспертов. Обязательный пересмотр настоящего Регламента с целью анализа и актуализации изложенной в ней информации должен осуществляться не реже одного раза в два года.

Приложение №1

**к Регламенту удостоверяющего Центра
АО «Фридом Банк Казахстан»**

ЖЕКЕ ТҰЛҒАНДАРДЫҢ ТІРКЕЛУ КУӘЛІКТЕРІН БЕРУ ҮШІН ӨТІНІШ / ЗАЯВЛЕНИЕ НА ВЫДАЧУ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ ОТ ФИЗИЧЕСКОГО ЛИЦА

Жеке сәйкестендіру нөмірі / Индивидуальный идентификационный номер:	
Тегі / Фамилия:	
Аты / Имя:	
Әкесінің аты / Отчество:	
Облыс атауы / Наименование области:	
Қала / Город:	
Электрондық поштаның адресі / Адрес электронной почты:	
Телефон:	
Тіркеу куәліктерінің әрекет ету мерзімі / Срок действия регистрационных свидетельств:	
Электрондық цифрлық қолтаңбаны қолдану аясы мен шектеулері туралы ақпарат / Информацию о сферах применения и ограничениях применения электронной цифровой подписи:	«Фридом Банк Қазақстан» АҚ сертификаттау орталығының қызметі туралы Ережеге (1.2.398.3.26.1) және «Freedom Bank Kazakhstan» АҚ сертификаттау орталығының тіркеу куәліктерін пайдалану саясатына сәйкес (1.2.398.3.26.2) / В соответствии с Регламентом деятельности удостоверяющего центра АО «Фридом Банк Казахстан» (1.2.398.3.26.1) и Политикой применения регистрационных свидетельств удостоверяющего центра АО «Фридом Банк Казахстан» (1.2.398.3.26.2): 1. Цифрлық қолтаңба / Цифровая подпись. 2. Бас тартпау / Неотрекаемость.
Электрондық цифрлық қолтаңбаның сәйкес жабық кілтін жасау үшін пайдаланылатын электрондық цифрлық қолтаңба құралдары туралы деректер, электрондық цифрлық қолтаңба алгоритмі стандартының белгіленуі және ашық кілттің ұзындығы / 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:	“ТУМАР-CSP”; ГОСТ 34.310-2004 (512 бит), Аутентификация – RSA 2048 бит)
Қосымша ақпарат алу үшін орын / Место для дополнительной информации:	«Фридом Банк Қазақстан» АҚ Куәландыру орталығына (бұдан әрі – КО) менің жеке деректерімді жинауға және өңдеуге, жеке ЭЦҚ кілтін КО бұлттық ЭЦҚ-да сақтауға келісімімді беремін, сондай-ақ талаптарды сақтауға міндеттенемін. Ереженің шарттары «Фридом Банк Қазақстан» АҚ Куәландыру орталығының қызметі, оның мәтіні

	https://pki.bankffin.kz/policy/regulations.pdf сілтемесінде орналастырылған. / Предоставляю согласие Удостоверяющему центру АО «Фридом Банк Казахстан» (далее – УЦ) на сбор и обработку моих персональных данных, на хранение закрытого ключа ЭЦП в облачной ЭЦП УЦ, а также обязуюсь выполнять условия Регламента деятельности удостоверяющего центра АО «Фридом Банк Казахстан», текст которого размещен по ссылке:https://pki.bankffin.kz/policy/regulations.pdf.
Күні / Дата:	« » _____ 20__ ж./г.

Осы құжатқа жіберілген динамикалық бір реттік кодты пайдалана отырып қол қойылды, уақыты _____ (күн мен уақыт), сағат белдеуі (UTC+5) телефон нөміріне + _____. / Настоящий документ подписан с использованием динамического одноразового (единовременного) кода ___ (номер кода), направленного ___ (дата (дд.мм.гг.), время ___ (час:мин.:сек) часовой пояс (UTC+5) на номер телефона + _____.

1-қосымша[1]
Жеке тұлғадан тіркеу куәліктерін беру туралы өтінішке
/ Приложение 1[1]
к Заявлению на выдачу регистрационных свидетельств от физического лица

Тіркеу куәлігінің нөмірі / Номер регистрационного свидетельства:	
ЭЦҚ ашық кілті / Открытый ключ ЭЦП:	

[1] *Жеке тұлғаның тіркеу куәлігін беру туралы өтінішке қол қойылғаннан және Банк куәландыру орталығының жеке ЭЦҚ кілтін бергеннен кейін қалыптастырылады. / Формируется после подписания Заявления на выдачу регистрационного свидетельства физического лица и выпуска закрытого ключа ЭЦП Удостоверяющего центра Банка.*

ЗАҢДЫ ТҰЛҒАДАН ТІРКЕУ КУӘЛІКТЕРІН БЕРУ ТУРАЛЫ ӨТІНІШ / ЗАЯВЛЕНИЕ НА ВЫДАЧУ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ ОТ ЮРИДИЧЕСКОГО ЛИЦА

Жеке сәйкестендіру нөмірі / Индивидуальный идентификационный номер:	
Бизнес-сәйкестендіру нөмірі / Бизнес-идентификационный номер:	
Компанияның атауы / Наименование организации:	
Заңды мекен-жайы / Юридический адрес:	
Тіркеу куәліктері атына берілген заңды тұлға басшысының сәйкестендіру деректері / Идентификационные данные руководителя юридического лица, на имя которого выдаются регистрационные свидетельства	
Тіркеу куәліктері атына берілген заңды тұлға басшысының жеке сәйкестендіру нөмірі / Индивидуальный идентификационный номер руководителя юридического лица, на имя которого выдаются регистрационные свидетельства:	
Тегі / Фамилия:	
Аты / Имя:	
Әкесінің аты / Отчество:	
Облыс атауы / Наименование области:	
Қала / Город:	
Электрондық поштаның адресі / Адрес электронной почты:	
Телефон:	
Тіркеу куәліктерінің әрекет ету мерзімі / Срок действия регистрационных свидетельств:	
Электрондық цифрлық қолтаңбаны қолдану аясы мен шектеулері туралы ақпарат / Информацию о сферах применения и ограничениях применения электронной цифровой подписи:	«Фридом Банк Қазақстан» АҚ сертификаттау орталығының қызметі туралы Ережеге (1.2.398.3.26.1) және «Freedom Bank Kazakhstan» АҚ сертификаттау орталығының тіркеу куәліктерін пайдалану саясатына сәйкес (1.2.398.3.26.2) / В соответствии с Регламентом деятельности удостоверяющего центра АО «Фридом Банк Казахстан» (1.2.398.3.26.1) и Политикой применения регистрационных свидетельств удостоверяющего центра АО «Фридом Банк Казахстан» (1.2.398.3.26.2): 1. Цифрлық қолтаңба / Цифровая подпись. 2. Бас тартпау / Неотрекаемость.
Электрондық цифрлық қолтаңбаның сәйкес жабық кілтін жасау үшін пайдаланылатын электрондық цифрлық қолтаңба құралдары туралы деректер, электрондық цифрлық қолтаңба алгоритмінің стандартының белгіленуі және ашық кілттің ұзындығы / Данные о средствах электронной цифровой подписи, используемых для создания соответствующего закрытого ключа электронной цифровой подписи, обозначение стандарта алгоритма электронной цифровой подписи и длины	«ТУМАР-CSP»; ГОСТ 34.310-2004 (512 бит), Аутентификация – RSA (2048 бит).

открытого ключа:	
Қосымша ақпарат алу үшін орын / Место для дополнительной информации:	
Күні / Дата:	« » _____ 20__ ж./г.

Бұл құжат электрондық цифрлық қолтаңба арқылы куәландырылған / Настоящий документ удостоверен посредством электронной цифровой подписи[2].

1-қосымша[3]
Заңды тұлғадан тіркеу куәліктерін беру туралы өтінішке
/ Приложение 1[1]
к Заявлению на выдачу регистрационных свидетельств от юридического лица

Тіркеу куәлігінің нөмірі / Номер регистрационного свидетельства:	
ЭЦҚ ашық кілті / Открытый ключ ЭЦП:	

[2] 2003 ж. 7-қаңтардағы N 370-II ҚРЗ 7-бабының 1-тармағына сәйкес электрондық цифрлық қолтаңба арқылы куәландырылған «Электрондық құжат және электрондық цифрлық қолтаңба туралы» қағаз тасымалындағы қол қойылған құжатқа тең. / Согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года N370-II «Об электронном документе и электронной цифровой подписи», удостоверенный посредством электронной цифровой подписи, равнозначен подписанному документу на бумажном носителе.

[3] Заңды тұлғаны тіркеу куәлігін беру туралы өтінішке қол қойылғаннан және Банк Куәландыру орталығының жеке ЭЦҚ кілтін бергеннен кейін қалыптастырылады. / Формируется после подписания Заявления на выдачу регистрационного свидетельства юридического лица и выпуска закрытого ключа ЭЦП Удостоверяющего центра Банка.

Приложение №2

к Регламенту удостоверяющего центра
АО «Фридом Банк Казахстан»

Жеке тұлғадан тіркеу куәлігін кері қайтарып алуға өтініш / Заявление на отзыв регистрационного свидетельства от физического лица

Жеке сәйкестендіру нөмірі / Индивидуальный идентификационный номер:	_____
Тегі / Фамилия:	_____
Аты / Имя:	_____
Әкесінің аты / Отчество:	_____
Электрондық поштаның адресі / Адрес электронной почты:	_____
Телефон:	_____
Тіркеу куәлігінің сәйкестендіру деректері / Идентификационные данные регистрационного свидетельства:	_____
Сериялық нөмірі / Серийный номер:	_____
Күні / Дата:	« » _____ 20__ ж./г.

Осы құжатқа жіберілген динамикалық бір реттік кодты пайдалана отырып қол қойылды, уақыты _____ (күн мен уақыт), сағат белдеуі (UTC+5) телефон нөміріне + _____. / Настоящий документ подписан с использованием динамического одноразового (единовременного) кода ___ (номер кода), направленного ___ (дата (дд.мм.гг.), время ___ (час:мин.:сек) часовой пояс (UTC+5) на номер телефона + _____.

Заңды тұлғадан тіркеу куәлігін қайтарып алуға өтініш / Заявление
на отзыв регистрационного свидетельства от юридического лица

Жеке сәйкестендіру нөмірі / Индивидуальный идентификационный номер:	_____
Бизнес-сәйкестендіру нөмірі / Бизнес-идентификационный номер:	_____
Ұйымның атауы / Наименование организации:	
Атына тіркеу куәліктері берілетін заңды тұлға қызметкерінің сәйкестендіру деректері / Идентификационные данные сотрудника юридического лица на имя которого выдается регистрационные свидетельства:	
Тегі / Фамилия:	_____
Аты / Имя:	_____
Әкесінің аты / Отчество:	_____
Электрондық поштаның адресі / Адрес электронной почты:	_____
Телефон:	_____
Тіркеу куәлігінің сәйкестендіру деректері / Идентификационные данные регистрационного свидетельства:	_____
Сериялық нөмірі / Серийный номер:	_____
Күні / Дата:	« » _____ 20__ ж./г.

Осы құжатқа жіберілген динамикалық бір реттік кодты пайдалана отырып қол қойылды, уақыты _____ (күн мен уақыт), сағат белдеуі (UTC+5) телефон нөміріне + _____. / Настоящий документ подписан с использованием динамического одноразового (единовременного) кода ___ (номер кода), направленного ___ (дата (дд.мм.гг.), время ___ (час:мин.:сек) часовой пояс (UTC+5) на номер телефона + _____.