**АО «Alatau City Bank»**
– конфиденциально

# ПОЛИТИКА
# применения регистрационных свидетельств Удостоверяющего центра АО «Alatau City Bank»

| | | |
|---|---|---|
| Владелец: | Департамент разработки продуктов | |
| Совладелец: | - | |
| Разработчик: | Департамент разработки продуктов | |
| Субъекты регулирования: | Департамент технологических решений<br>Департамент сопровождения ИС<br>Департамент IT Governance<br>Департамент управления инфраструктурой<br>Департамент разработки продуктов | |
| Утвержден: | Советом директоров<br>(протокол № 25/12/25-01) | от «25» декабря 2025г. |
| ВД, признаваемые утратившими силу: | Политика применения регистрационных свидетельств Удостоверяющего центра | Утверждена Советом директоров<br>АО «Jusan Bank»<br>(протокол № 02/06/23-01<br>от 02.06.2023г.) |

**Содержание**

## Глава 1. Общие положения

1. Настоящая Политика применения регистрационных свидетельств удостоверяющего центра АО «Alatau City Bank» (далее – Политика) определяет регламент и механизмы работы Удостоверяющего центра АО «Alatau City Bank» (далее – УЦ) в части управления регистрационными свидетельствами, а также общие положения, включая цели и задачи, область применения, принципы функционирования системы регистрации и управления регистрационными свидетельствами. Политика также устанавливает стратегию УЦ, в области управления процессом выдачи регистрационных свидетельств, общие правила их применения, процедуры проверки, а также способы использования регистрационных свидетельств.

2. Политика разработана в соответствии с законодательством Республики Казахстан (далее – РК) – Закон РК «Об электронном документе и электронной цифровой подписи», Закон РК «О персональных данных и их защите», Правила создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре, утвержденные приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НҚ, Правила выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром, за исключением корневого удостоверяющего центра Республики Казахстан, удостоверяющего центра государственных органов, национального удостоверяющего центра Республики Казахстан и доверенной третьей стороны Республики Казахстан, утвержденные приказом Министра по инвестициям и развитию Республики Казахстан от 23 декабря 2015 года № 1231, Правила проверки подлинности электронной цифровой подписи утвержденные приказом Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187, и иными нормативно-правовыми актами РК, в целях обеспечения функционирования УЦ с учетом международных отраслевых рекомендаций RFC 3647 «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework» (стандарт, определяющий форматы данных и процедуры распределения открытых ключей с помощью регистрационного свидетельства с ЭЦП X.509).

3. Целью Политики является определение общих требований к процедурам и условиям предоставления УЦ услуг, связанных с жизненным циклом регистрационных свидетельств УЦ.

4. Основными задачами Политики является осуществление контроля:

1) за соблюдением требований законодательства РК и внутренних документов Банка при осуществлении деятельности УЦ;

2) за надлежащим применением ЭЦП при подписании электронных документов владельцами регистрационных свидетельств.

5. Требования Политики обязательны для исполнения всеми участниками инфраструктуры открытых ключей УЦ, включая работников, и внешних контрагентов, использующих регистрационные свидетельства, выданные УЦ.

## Глава 2. Глоссарий

6. В Политике используются следующие понятия, определения и сокращения:

1) аппаратный криптографический модуль (Hardware Security Module (далее – HSM) – аппаратный криптографический модуль, предназначенный для шифрования информации и управления открытыми и закрытыми ключами ЭЦП;

2) аутентификация – процедура проверки подлинности личности или учетных данных пользователя, для обеспечения доступа путем определения соответствия предъявленных (вводимых) реквизитов доступа, имеющимся на информационном активе и (или) объекте информационно-коммуникационной инфраструктуры;

3) Банк – АО «Alatau City Bank»;

4) бизнес-клиент – юридическое лицо (независимо от организационно-правовой

формы и формы собственности, включая обособленные подразделения юридического лица (филиалы и представительства), иностранная структура без образования юридического лица, иностранное дипломатическое и консульское представительство, индивидуальные предприниматели (крестьянские (фермерские) хозяйства), или лица, занимающиеся в установленном законодательством Республики Казахстан порядке частной практикой (частные нотариусы, частные судебные исполнители, адвокаты и профессиональные медиаторы), финансовые управляющие, открывшие или намеревающиеся открыть банковский счет в Банке;

5) ВД – внутренние документы Банка;

6) владелец регистрационного свидетельства (далее – владелец) – клиент Банка - физическое лицо/бизнес-клиент, на имя которого УЦ выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве;

7) жизненный цикл – выдача, хранение и прекращение срока действия (отзыв), публикация выпущенных регистрационных свидетельств УЦ;

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

9) заявитель – клиент Банка – физическое лицо, бизнес-клиент подавший(-ее) документы в УЦ для выдачи или отзыва регистрационного свидетельства;

10) идентификация –процесс (или результат процесса), который устанавливает идентичность физического лица/ бизнес-клиента (показывающий, что данное лицо является однозначно определенным реально существующим лицом);

11) официальный сайт Банка – это веб-ресурс, принадлежащий Банку и предназначенный для предоставления информации о его деятельности, продуктах и услугах, а также для взаимодействия с клиентами по адресу www.alataucitybank.kz;

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

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

14) 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 посредством не менее двух факторов аутентификации, одним из которых является биометрическая;

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

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

17) OCSP – сервис для получения информации о статусе регистрационных свидетельств, выпущенных УЦ (согласно рекомендациям RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP», онлайн протокол статуса сертификатов интернет-инфраструктуры открытых ключей ЭЦП X.509));

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

19) Регламент деятельности удостоверяющего центра (далее – Регламент) – ВД, регламентирующий порядок организации основной деятельности УЦ, осуществляемой в соответствии с Политикой;

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

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

22) участники инфраструктуры открытых ключей (далее – участник ИОК) – работники УЦ, отвечающие за обслуживание клиентов, а также владельцы регистрационных свидетельств;

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

24) центр сертификации – программно-аппаратный комплекс УЦ для выдачи, обслуживания и отзыва регистрационного свидетельства, своевременный импорт СОРС, действующий в соответствии с законодательством РК;

25) центр регистрации – информационная система Банка, в том числе мобильное приложение Банка, посредством которой Банком предоставляются услуги дистанционного банковского обслуживания, принимающая заявления от владельца на выпуск и отзыв регистрационного свидетельства, а также осуществляющая проверку, идентификацию и аутентификацию заявителей;

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

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

Иные специфические термины и сокращения, используемые по тексту Политики, применяются в соответствии со значением, закрепленным в законодательстве РК, во ВД по деятельности УЦ или принятым в международной банковской практике.

Все ссылки на части, разделы, главы, параграфы, пункты, приложения в тексте Политики без указания названия документа относятся к настоящей Политики.

## Глава 3. Назначение регистрационных свидетельств

7. УЦ выдает, регистрирует, отзывает, хранит регистрационные свидетельства, ведет хранилище регистрационных свидетельств, выданных в установленном порядке, а также публикует регистрационные свидетельства УЦ на официальном сайте Банка и нормативные документы, включая Регламент оказания услуг, политики безопасности, процедуры сертификации и управления ключами, а также другие данные о своих сервисах.

8. Не допускается использование владельцами регистрационных свидетельств, выданных им в УЦ, для целей, связанных с управлением источниками повышенной опасности включая ядерные объекты, системы контроля вооружений и другие аналогичные технологии. Также запрещается использование этих свидетельств в случаях, которые могут привести к ущербу для здоровья и жизни персонала, а также к вреду окружающей среде.

9. Не допускается использование регистрационных свидетельств, выпущенных УЦ, способами, противоречащими законодательству РК, Политике УЦ, Регламенту деятельности УЦ.

10. Регистрационные свидетельства владельцев УЦ предназначены для обеспечения работы с программным обеспечением доверяющих сторон, включая аутентификацию, шифрование и подтверждение подлинности данных.

## Глава 4. Хранилище Удостоверяющего центра и публикация в нем данных

### §1. Хранилище и публикация

11. Составной частью центра сертификации УЦ является хранилище данных (реестр или каталог), в котором содержится информация о регистрационных свидетельствах, включая выданные, приостановленные и отозванные регистрационные свидетельства. УЦ использует это хранилище в качестве справочника информации при предоставлении своих основных сервисов, таких как аутентификация, проверка подлинности регистрационных свидетельств, управление их статусами и ведение журналов аудита.

12. УЦ ведет раздел на официальном сайте Банка, в котором публикует информацию о выпуске/отзыве регистрационных свидетельств УЦ, ВД по деятельности УЦ, включая Политику УЦ, Регламент УЦ, а также другие сведения о своих сервисах (далее – Сведения).

### §2. Периодичность актуализации данных в хранилище

13. УЦ публикует каждое вновь выпущенное регистрационное свидетельство в хранилище.

14. В случае отзыва регистрационного свидетельства УЦ удаляет его в порядке, определенном в Регламенте.

15. Действие регистрационного свидетельства прекращается по истечении срока, на который оно было выдано УЦ, и УЦ удаляет его в порядке, определенном в Регламенте.

### §3. Контроль доступа к хранилищу

16. УЦ создает ключи ЭЦП по обращению заявителей принимая меры для защиты закрытых ключей ЭЦП от неправомерного доступа с использованием шифрования, аппаратных модулей безопасности и ограничения доступа, в соответствии с ВД, регламентирующими обеспечение требований информационной безопасности (далее – ИБ), Регламентом работы с ключами ЭЦП, и ВД, регламентирующими обеспечение ИБ ИС УЦ.

17. УЦ для предотвращения утери, модификации, подделки находящихся на хранении открытых ключей и/или закрытых ключей ЭЦП принимает меры, основанные на законодательстве РК и лучших международных практиках, которые помогут обеспечить надежную защиту ключей ЭЦП и соответствие требованиям законодательства РК и стандартов.

18. Сведения, публикуемые на официальном сайте Банка с правами «только для чтения», включают регистрационные свидетельства, ВД по деятельности УЦ (Политику УЦ, Регламент, Правила и другое), список отозванных регистрационных свидетельств, описание услуг УЦ, контактную информацию и инструкции для пользователей.

## Глава 5. Идентификация и аутентификация

### §1. Требования к именам владельцев

19. УЦ выпускает сертификаты, соответствующие стандартам X.509 версии 3 (рекомендации ITU-T) и RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile». В сертификате указывается отличительное имя (DN) в поле Subject, оформленное по правилам стандарта X.501 ITU-T. Это DN содержит персональные данные, которые позволяют однозначно идентифицировать физическое или юридическое лицо — владельца сертификата. Таким образом, DN определяет владельца сертификата и его закрытого ключа, а также область применения данного сертификата, выданного УЦ.

### §2. Первоначальная идентификация

20. Первоначальная идентификация заявителя и любая последующая процедура, требующая идентификации владельца регистрационного свидетельства, проводится в соответствии с Регламентом. Подача заявлений на выпуск и отзыв регистрационных свидетельствах осуществляется в режиме онлайн через системы дистанционного банковского обслуживания с применением многофакторной аутентификации, включая биометрическую.

## Глава 6. Общие требования к жизненному циклу регистрационных свидетельств

### §1. Заявление на выпуск (выдачу) регистрационного свидетельства

21. Заявление на выпуск (выдачу) регистрационного свидетельства имеют право подавать физические лица/бизнес-клиенты.

22. Принципы оформления заявлений на выпуск регистрационного свидетельства определены Регламентом.

### §2. Обработка заявления на выпуск (выдачу) регистрационного свидетельства

23. Центр регистрации обрабатывает заявление на выпуск регистрационного свидетельства в соответствии с законодательством РК по вопросам электронного документа и электронной цифровой подписи.

24. Срок рассмотрения и обработки заявлений на выпуск регистрационных свидетельств определяется Регламентом.

25. Зарегистрированное заявление отклоняется УЦ в случаях, установленных законодательством РК по вопросам электронного документа и электронной цифровой подписи и Регламентом.

### §3. Выпуск регистрационных свидетельств

26. Каждое регистрационное свидетельство создается УЦ по факту регистрации и успешной обработки отдельного заявления на выпуск регистрационного свидетельства в центре регистрации.

27. Принципы и основные этапы выпуска регистрационного свидетельства заявителю определены в Регламенте.

### §4. Использование регистрационных свидетельств и ключевых пар

28. Необходимые условия использования регистрационных свидетельств и пар ключей определены Регламентом.

29. Политика и Регламент деятельности УЦ, являющиеся ВД, доводятся до других лиц путем публикации на официальном сайте Банка, с включением ссылки в формы заявлений и электронные формы согласия, а также предоставляются в отделениях Банка в виде печатных экземпляров по запросу.

### §5. Смена ключей и обновление сроков действия в регистрационных свидетельствах

30. УЦ не предоставляет услуги по обновлению сроков действия открытых ключей в регистрационных свидетельствах. Перевыпуск ключей в регистрационных свидетельствах осуществляется в соответствии с Регламентом.

### §6. Изменение данных в регистрационных свидетельствах

31. УЦ не предоставляет услуги по изменению данных в регистрационных свидетельствах.

### §7. Отзыв регистрационных свидетельств

32. Регистрационные свидетельства, выпущенные УЦ, могут быть отозваны УЦ по основаниям, установленным законодательством РК по вопросам электронного документа и электронной цифровой подписи и в Регламенте.

## Глава 7. Виды контроля Удостоверяющего центра

### §1. Физический контроль

33. Условия размещения оборудования центра сертификации в основном и резервном центрах обработки данных соответствуют требованиям, действующим в РК к системам бесперебойного функционирования технических средств и требованиям обеспечения ИБ, а также определенным Регламентом.

34. Все операции (генерация, хранение, использование, резервное копирование, восстановление и уничтожение ключей) с ключами УЦ проводятся УЦ только в охраняемых помещениях, в условиях, где затруднены и фиксируются любые попытки несанкционированного доступа, использования или раскрытия конфиденциальной информации. Допускается дистанционное осуществление деятельности УЦ при условии соблюдения требований законодательства РК, и ВД Банка, включая, но не ограничиваясь ВД, регламентирующих порядок обеспечения требований ИБ.

### §2. Операционный контроль

35. Физический и логический доступ к оборудованию центра сертификации разделены процедурно.

36. Для физического доступа к процедурам настройки и обслуживания аппаратных криптографических модулей (Hardware Security Module (далее – HSM) и их ключевого материала требуется участие минимум двоих уполномоченных работников Банка в соответствии с Регламентом.

37. Процедуры обработки логических запросов к центру сертификации автоматизированы на уровне прикладного программного обеспечения, с контролем полномочий инициаторов запроса.

### §3. Управляющий контроль

38. Все функции, обеспечивающие надлежащую работу УЦ, выполняются работниками Банка в соответствии с полномочиями, определенными Регламентом.

39. Допускается привлечение контрагентов в рамках договоров поставки и технической поддержки аппаратного и программного обеспечения центра сертификации УЦ. Все работы привлеченных контрагентов выполняются строго в присутствии работников Банка.

40. Привлечение третьих лиц на основании договоров гражданско-правового характера к выполнению функций, обеспечивающих работу УЦ, не допускается.

### §4. Процедуры контрольного протоколирования

41. Обработка запросов (на выдачу и отзыв регистрационных свидетельств, проверку состояния регистрационных свидетельств и другие) УЦ осуществляется с обязательным контрольным протоколированием, включающим регистрацию инициатора запроса.

42. Типы событий, подлежащих протоколированию:

УЦ обеспечивает протоколирование следующих событий:

- запрос на выпуск сертификата;
- запрос на отзыв сертификат;
- формирование закрытого ключа ЭЦП облачной ЭЦП;
- использование закрытого ключа ЭЦП облачной ЭЦП;
- удаление (стирание) закрытого ключа ЭЦП облачной ЭЦП.

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

При протоколировании действий записывается следующая информация:

- дата, время;
- DN имя владельца сертификата;
- событие.

43. Протоколы событий ежедневно преобразуется в хэш, и данные хэш хранятся в цепочке событий блокчейн. Применяемая для этого блокчейн доступна на официальном сайте Банка.

### §5. Смена ключей Удостоверяющего центра

44. Смена ключей УЦ осуществляется в соответствии с эксплуатационно-технической документацией аппаратных криптографических модулей (HSM) УЦ в соответствии с Регламентом.

### §6. Восстановление функционирования в случае чрезвычайных происшествий или компрометации

45. На случай чрезвычайных и иных происшествий, влекущих прерывание функционирования сервисов УЦ, УЦ действует в соответствии с Инструкцией по действиям работников Удостоверяющего центра во внештатных, кризисных ситуациях, Инструкцией по резервному копированию, архивированию и восстановлению данных информационных ресурсов Удостоверяющего центра, а также ВД, регламентирующим правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации. Резервное копирование закрытого ключа УЦ происходит в соответствии с эксплуатационной документацией HSM модулей и СКЗИ по схеме n из m. Резервная копия закрытого ключа УЦ хранится отдельно от криптографического модуля в зашифрованном архиве.

46. Приоритетом восстановления функционирования является возобновление основных сервисов УЦ по публикации сведений о статусе регистрационных свидетельств, выпуска и отзыва регистрационных свидетельств.

### §7. Ведение архива

47. УЦ ведет архив, в котором хранит письменные и электронные документы, определенные Регламентом.

48. Архив УЦ ведется на постоянной основе в соответствии с регламентированными сроками и требованиями законодательства РК.

## Глава 8. Технический контроль безопасности ключей

### §1. Генерация и установка

49. Генерация ключей центром сертификации проводится только с помощью СКЗИ, криптографическая стойкость которых подтверждена сертификатом соответствия действующему в РК стандарту, который определяет общие технические требования к средствам криптографической защиты информации (далее – Стандарт).

50. Генерация ключей центром сертификации проводится только несколькими уполномоченными (в соответствии с должностными обязанностями) и предварительно обученными работниками УЦ в соответствии с Регламентом.

### §2. Защита закрытых ключей и инженерные контроли криптографических модулей

51. Меры защиты закрытых ключей УЦ от разглашения, искажения, подмены и несанкционированного использования определены в Регламенте.

52. Закрытые ключи ЭЦП облачной ЭЦП генерируются строго внутри HSM. Закрытый ключ не извлекается из HSM в открытом виде.

При этом HSM:

1) соответствует не ниже, чем 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. Иные аспекты управления ключами

53. Все открытые ключи, заверенные регистрационным свидетельством, которое когда-либо выпустил УЦ, подлежат архивированию в составе этих регистрационных свидетельств.

54. Порядок управления ключами определяется Регламентом.

### §4. Контроль безопасности вычислительных ресурсов

55. Вычислительные ресурсы, программное обеспечение и данные центра сертификации защищаются от несанкционированного доступа в соответствии с ВД о процедурах обеспечения ИБ и Регламентом, включающими контроль доступа, шифрование, мониторинг, защиту от вредного ПО, резервное копирование, обучение сотрудников и реагирование на инциденты.

### §5. Контроль управления развитием и безопасностью

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

## Глава 9. Профили регистрационных свидетельств, CORC и OCSP

### §1. Профили регистрационных свидетельств

57. УЦ выпускает регистрационные свидетельства в соответствии требованиям стандарта X.509 и рекомендациям стандарта RFC 5280.

58. Основные поля, содержащиеся в регистрационных свидетельствах, вместе с требованиями к их содержанию определяются в соответствии с Регламентом.

### §2. Профили списка отозванных регистрационных свидетельств

59. УЦ формирует и публикует на официальном сайте Банка списки отозванных регистрационных свидетельств в соответствии со стандартом ITU-T X.509 (версии 3 и RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile»).

60. Основные поля и расширения, содержащиеся в списках отозванных регистрационных свидетельств, вместе с требованиями к их содержанию определяются в соответствии с Регламентом.

### §3. Профиль сервиса OCSP

61. Сервис OCSP для получения информации о статусе регистрационных свидетельств, выпущенных УЦ, предоставляется в соответствии с Регламентом.

## Глава 10. Проверка деятельности

62. Уполномоченный государственный орган вправе осуществлять плановые/внеплановые проверки деятельности УЦ.

## Глава 11. Прочие вопросы

### §1. Тарифы

63. Услуги УЦ не тарифицируются и не оплачиваются.

### §2. Защита персональных данных участников

64. УЦ обеспечивает защиту персональных данных участников ИОК в соответствии с законодательством РК в области персональных данных и их защиты.

### §3. Права интеллектуальной собственности

65. В своей деятельности УЦ использует программное обеспечение в соответствии с Регламентом. Порядок использования программного обеспечения определяется условиями лицензионных договоров, заключенных Банком и обладателями соответствующих прав на программное обеспечение.

### §4. Гарантии и заверения

66. УЦ в своей деятельности выполняет условия собственных гарантий и заверений в отношении владельцев и доверяющих сторон регистрационных свидетельств, при этом заверения владельца, изложенные в Регламенте, выполняются самим владельцем.

### §5. Уведомления и связь с участниками

67. Участники ИОК для связи друг с другом используют каналы, в соответствии с Регламентом.

### §6. Разрешение споров

68. Споры между участниками ИОК: между владельцами и пользователями регистрационных свидетельств (владельцами и доверяющими сторонами), а также между владельцем или доверяющей стороной с одной стороны, и Удостоверяющим центром, с другой стороны, - разрешаются в соответствии с положениями договоров, действующих между сторонами, и/или законодательством РК.

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

## Глава 12. Ответственность

70. Ответственность УЦ, владельцев и пользователей регистрационных свидетельств (владельцев и доверяющих сторон) ограничена законодательством РК.

71. Ответственность за неисполнение и/или ненадлежащее исполнение Политики возлагается на работников и руководителей структурных подразделений Головного Банка и обособленных подразделений Банка, участвующих в процессе обслуживания центра регистрации, центра сертификации, УЦ.

72. Общий контроль за организацией и поддержание УЦ, центра регистрации, осуществляется подразделениями Банка, участвующими в процессе обслуживания центра регистрации, УЦ, как участниками первой линии защиты системы внутреннего контроля Банка, регламентированной Политикой внутреннего контроля Банка. Общий контроль функционирования центра регистрации, УЦ осуществляется на постоянной основе.

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

## Глава 13. Конфиденциальность

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

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

76. Регистрационные свидетельства, выпускаемые УЦ, включая данные, позволяющие идентифицировать владельца ЭЦП, и информация об их отзыве или ином статусе, не являются и не рассматриваются в качестве конфиденциальной информации.

## Глава 14. Заключительные положения

77. Политика может быть изменена по мере пересмотра основных задач УЦ, появления/сокращения функций, в соответствии с законодательством РК, а также в иных случаях.

78. Политика вводится в действие по истечении 10 (десяти) рабочих дней (срок ввода в действие ВД может быть изменен в сторону уменьшения на усмотрение разработчика, владельца, совладельца ВД) с даты публикации на официальном сайте Банка, если решением Совета директоров не установлен иной срок введения ее в действие.

79. Решение о признании утраты силы Политики вступают в силу в день ввода в действие новой редакции Политики или замещающего его внутреннего документа, или по истечении 10 (десяти) рабочих дней со дня принятия решения Советом директоров, если не установлен иной срок решением Совета директоров.

80. Положения, не урегулированные Политикой, регулируются законодательством РК и ВД Банка.

81. В случае изменения законодательства РК и возникновения противоречий отдельных положений Политики законодательству РК, такие положения Политики утрачивают силу, и работники Банка руководствуются в своей деятельности законодательством РК до соответствующей актуализации и/или внесения изменений в Политику.