АО «Alatau City Bank»
Степень конфиденциальности – для служебного пользования

РЕГЛАМЕНТ
деятельности Удостоверяющего центра
АО «Alatau City Bank»

Владелец:	Департамент разработки продуктов	
Совладелец:	-	
Разработчик:	Департамент разработки продуктов	
Субъекты регулирования:	Департамент технологических решений Департамент сопровождения ИС Департамент IT Governance Департамент управления инфраструктурой Департамент разработки продуктов Департамент безопасности	
Утвержден:	Правлением АО «Alatau City Bank» (протокол № 122–25)	от «11» декабря 2025г.
ВД, признаваемые утратившими силу:	Правила деятельности Удостоверяющего центра	Утверждены Правлением АО «Jusan Bank» (протокол № 61–23 от 02.06.2023г.)

Содержание

Глава 1. Общие положения

1. Настоящий Регламент деятельности удостоверяющего центра АО «Alatau City Bank» (далее – Регламент) определяет правила, механизмы и условия предоставления и использования услуг удостоверяющего центра АО «Alatau City Bank» (далее – УЦ), включая права, обязанности и ответственность участников УЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, включая выпуск, использование и отзыв регистрационных свидетельств.

2. Регламент разработан:

1) в соответствии с законодательством Республики Казахстан (далее – РК), в том числе:

а) Законом РК «Об электронном документе и электронной цифровой подписи»;

б) Законом РК «О персональных данных и их защите»;

в) Правилами создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре, утвержденные приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27.10.2020 года № 405/НҚ;

г) Правилами проверки подлинности электронной цифровой подписи, утвержденные приказом Министра по инвестициям и развитию Республики Казахстан от 09.12.2015 года № 1187;

д) 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 Республики Казахстан от 23.12.2015 года № 1231;

е) СТ РК 1073-2007. Средства криптографической защиты информации. Общие требования.

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

3. Регламент регулирует меры, реализуемые УЦ при обеспечении набора сервисов, который определен Политикой применения регистрационных свидетельств удостоверяющего центра АО «Alatau City Bank» (далее – Политика УЦ) и включает в себя, но не ограничивается выпуском, управлением и отзывом регистрационного свидетельства.

4. Регламент определяет порядок и процедуры:

1) выпуска и дальнейшего обслуживания выпущенного УЦ регистрационного свидетельства;

2) выполнения функций (работы сервисов) УЦ;

3) обеспечения информационной безопасности и управления центральными компонентами инфраструктуры открытых ключей, включая криптографическую защиту данных, контроль физического и сетевого доступа, мониторинг и управление инцидентами, а также резервное копирование и восстановление;

4) процедуры проверки, связанные с выпуском и дальнейшим обслуживанием регистрационного свидетельства, которые выпускает УЦ.

5. С момента подписания заявления на выпуск регистрационного свидетельства клиент Банка или уполномоченное лицо бизнес-клиента, использующей сервисы УЦ, обязаны соблюдать требования настоящего Регламента, ссылка на который указана в заявлении.

6. Регистрационное свидетельство УЦ применимо для следующих целей:

1) подписание электронной цифровой подписью электронных документов (договоров/соглашений, заявлений и прочих документов в целях банковского обслуживания,

в том числе получения/обслуживания/погашения банковских займов, и в иных целях, разрешенных законодательством РК), подписание которых реализовано в информационных системах Банка;

2) проверка электронной цифровой подписи;

3) аутентификация владельцев.

7. Объектный идентификатор Политики УЦ соответствует требованиям, регулирующим функции следующих категорий работников УЦ:

1) Администратор УЦ – Департамент сопровождения ИС, выполняющий функции: разработки шаблонов (настройка конфигурации в приложении по требованию бизнес владельца УЦ), выдачу регистрационного свидетельства, проверки работы центра сертификации, обеспечение надлежащего функционирования центра сертификации;

2) Системный администратор УЦ/Дежурный УЦ – Департамент управления инфраструктурой, контролирующий/обслуживающий/ выполняющий функции: консоль, сеть, базу данных, сопровождение запуска Hardware Security Module, обеспечение отказоустойчивости в рамках компетенции, предоставление доступов к серверам УЦ, бэкап HSM, мониторинга центра сертификации/программного обеспечения УЦ;

3) бизнес-владелец УЦ – Департамент разработки продуктов, являющейся владельцем основного бизнес-процесса УЦ по выпуску регистрационного свидетельства, и выполняющий функции разработки Регламента, Политики, согласование предоставления доступов работникам Банка, разбор конфликтных ситуаций.

8. Полный перечень объектных идентификаторов политики в клиентском регистрационном свидетельстве приведен на официальном сайте Банка.

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

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

11. Требования Регламента обязательны для исполнения бизнес-владельцем УЦ и бизнес-владельцем информационной системы, Системным администратором УЦ/Дежурным УЦ и Администратором УЦ.

Глава 2. Глоссарий

12. В Регламенте используются следующие основные 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 владельцев, 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-владелец ИС – подразделение Банка, являющееся владельцем основного бизнес-процесса информационной системы Банка/системы дистанционного банковского обслуживания (центра регистрации), который автоматизирует информационный актив. При необходимости внесения изменений/доработок в центр регистрации бизнес-владелец ИС обращается в подразделение Банка, ответственное за техническое сопровождение данной системы, в соответствии с ВД, регламентирующим порядок взаимодействия при разработке, доработке и внедрении информационных систем, подсистем, модулей;

5) 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, иностранные дипломатические и консульские представительства, 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;

6) блокчейн – информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе данных на базе цепочки взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования;

7) ВД – внутренние документы Банка;

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

9) данные активации – это данные, необходимые для выполнения криптографических операций, требующие защиты, но не являющиеся криптографическими ключами. К данным активации относятся персональные идентификационные номера (далее – PIN), парольные фразы, компоненты разделенного ключа, биометрические параметры и другие аналогичные сведения, используемые для аутентификации и управления доступом к криптографическим средствам;

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

11) 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;

12) заявитель – клиент Банка – физическое лицо, бизнес-клиент, подавший документы в удостоверяющий центр для выдачи или отзыва регистрационного свидетельства;

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

а) установление соответствия предъявленного лицом имени реально существующему лицу;

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

14) 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;

15) 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;

16) инфраструктура открытых ключей (далее – ИОК) – совокупность технических, программных, материальных, кадровых и иных ресурсов, а также распределённых служб и компонентов, используемых для реализации криптографических задач, включая аутентификацию, шифрование, контроль целостности и подтверждение авторства на основе криптосистем с открытым ключом, обеспечивающая самостоятельное управление открытыми ключами, посредством которых обеспечивается выполнение указанных функций;

17) контрольный протокол – это зафиксированные в установленном порядке данные о выполненных операциях в УЦ, предназначенные для мониторинга, проверки и подтверждения корректности и безопасности процессов, а также для аудита и расследования инцидентов;

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

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

20) 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;

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

22) 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;

23) офицер безопасности УЦ – работник Департамента защиты информационных систем, выполняющий функции хранения токенов HSM в своей части;

24) Политика УЦ – которая определяет общие положения, включая цели, задачи, область применения, а также 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;

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

26) Регистр регистрационных свидетельств – систематизированный перечень – выпущенных и отозванных регистрационных свидетельств с указанием основных реквизитов владельцев и сроков их действия;

27) 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;

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

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

30) участники инфраструктуры открытых ключей ЭЦП (далее – участники ИОК) – работники УЦ, ответственные за обслуживание клиентов, а также владельцы регистрационных свидетельств;

31) Удостоверяющий центр (далее – УЦ) – Департамент разработки продуктов, выполняющее функции по удостоверению соответствия открытого ключа электронной цифровой подписи (ЭЦП) соответствующему закрытому ключу, а также подтверждающее достоверность регистрационного свидетельства, выданного клиенту, в соответствие с требованиями законодательства Республики Казахстан «Об электронном документе и

электронной цифровой подписи»;

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

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

34) 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. При недоступности сервиса центра регистрации выпуск и отзыв регистрационных свидетельств УЦ не осуществляется;

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

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

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

Иные специфические термины и сокращения, используемые по тексту Регламента, применяются в соответствии со значением, закрепленным в законодательстве РК, во внутренних документах Банка или закрепленным в международной банковской практике;

38) LDAP (Lightweight Directory Access Protocol) – стандартный протокол, применяемый для доступа, поиска и управления данными в распределенных каталогах. В УЦ LDAP используется для хранения и предоставления информации о сертификатах открытых ключей, их статусах, а также для аутентификации и авторизации владельцев при работе с сервисами электронной цифровой подписи.

Все ссылки на части, разделы, главы, параграфы, пункты, приложения в тексте Регламента без указания названия документа относятся к настоящему Регламенту.

Глава 3. Виды и способы использования регистрационных свидетельств

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

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

14. УЦ выпускает регистрационное свидетельство, которое содержит информацию о сферах применения и ограничениях применения ЭЦП, и соответственно, разные профили, которые отражаются в расширении «keyUsage» и/или «extendedKeyUsage» регистрационного свидетельства.

15. Способы использования регистрационных свидетельств УЦ не должны

противоречить законодательству РК и требованиям Регламента.

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

Глава 4. Хранилище и публикация данных (регистрационного свидетельства)

§1. Хранилище

17. УЦ на официальном сайте Банка с целью уведомления владельцев регистрационных свидетельств и их доверяющих сторон о выпуске регистрационного свидетельства и размещения СОРС, а также в соответствии с Политикой публикует:

1) Политику регистрационных свидетельств;
2) Регламент;
3) регистрационные свидетельства УЦ;
4) ссылки для доступа к СОРС;
5) цепочка событий блокчейн.

18. Официальным уведомлением УЦ владельцев регистрационных свидетельств и их доверяющих сторон о выпуске регистрационного свидетельства и размещения СОРС является публикация в хранилище, которая доступна на официальном сайте Банка, а также сохранение его в центре регистрации. Дополнительно официальный сайт Банка используется для размещения иной важной информации УЦ, сведений, в целях уведомления владельцев регистрационных свидетельств (доверяющих сторон).

§2. Публикация в хранилище информации о регистрационных свидетельствах

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

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

21. Любые исключения из этих требований (обязательного использования Lightweight Directory Access Protocol v.3, версия 3 и обеспечения онлайн-доступа), в случае их возникновения, должны быть включены в Регламент и опубликованы в свободном доступе для владельцев регистрационных свидетельств и доверяющих сторон.

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

§3. Периодичность актуализации данных в хранилище

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

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

25. Срок действия регистрационных свидетельств УЦ:

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

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

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

27. При отзыве УЦ регистрационное свидетельство автоматически удаляется из списка действующих регистрационных свидетельств хранилища и переносится в СОРС. Срок

хранения отозванных регистрационных свидетельств в регистре регистрационных свидетельств (хранилище) составляет не менее 5 (пяти) лет. Далее отозванные регистрационные свидетельства поступают на архивное хранение в соответствии с требованиями законодательства РК. Контроль за корректностью процесса возлагается на бизнес-владельца УЦ. СОРС публикуется на официальном сайте Банка.

28. Регистрационные свидетельства, которые не были отозваны, но прекратили действие в связи с истечением срока действия, автоматически удаляются из хранилища и переносятся в архив, где хранятся не менее 5 (пяти) лет.

29. Сведения об отозванных регистрационных свидетельствах с истекшим сроком действия удаляются из списков отозванных регистрационных свидетельств по факту истечения их срока действия, не реже одного раза в неделю в соответствии с расписанием, установленным настройками центра сертификации. Ответственность за настройку расписания и его согласование возлагается на бизнес-владельца УЦ, настройки расписания осуществляет Администратор УЦ.

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

31. В условиях отсутствия событий отзыва регистрационных свидетельств новый СОРС формируются и выпускаются автоматически на еженедельной основе в соответствии с расписанием, установленным настройками центра сертификации.

§4. Контроль доступа к хранилищу

32. Доступ к данным из хранилища предоставляется УЦ к обслуживаемым ИС Банка в рамках логического взаимодействия, по заявкам, оформленным согласно внутреннему документу процесса контроля доступа к исходным кодам информационных систем (согласование с ИБ и владельцами систем). При необходимости физического размещения оборудования УЦ или подключения к инфраструктуре Банка, доступ обеспечивается в порядке, установленном документом по правилам монтажа и размещения систем контроля и управления доступом.

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

34. Удаление/добавление данных в(из) хранилище(-а) осуществляется Администратором УЦ, Системным администратором на основании заявки в Service Desk от бизнес-владельца УЦ.

35. Бизнес-владелец УЦ обеспечивает защиту хранилища от несанкционированного доступа с применением установленных в Банке организационных и технических мер информационной безопасности. Сведения, предназначенные для участников ИОК, размещаются на официальном сайте Банка в открытом доступе в режиме «только для чтения», без возможности их изменения или удаления со стороны любых третьих лиц (посетителей сайте Банка). УЦ обеспечивает публикацию следующей информации на официальном сайте Банка:

- сертификат УЦ по алгоритму СТ РК ГОСТ Р 34.10-2015;
- хранилище сертификатов;
- Регламент деятельности УЦ;
- Политика применения регистрационных свидетельств УЦ;
- СОРС.

36. В случае превышения нагрузок на сервис доступа к хранилищу УЦ автоматически вводит временные ограничения доступа.

Ограничения могут вводиться также при обнаружении кибератак, иных угроз информационной безопасности, технических перебоев в предоставлении сервисов, а также при наличии обоснованных подозрений в их возникновении.

Данный порядок регламентируется ВД Банка, включая, но не ограничиваясь ВД,

регламентирующим порядок разграничения прав доступов, договорами с клиентами, внутренними регламентами взаимодействия подразделений, а также регламентом работы УЦ.

37. Временные ограничения доступа к хранилищу применяются в соответствии с требованиями Национального Банка РК, включая постановление Правления Национального Банка РК № 34 «Об утверждении требований к безопасности и бесперебойности работы информационных систем банков, филиалов банков, нерезидентов РК и организаций, осуществляющих отдельные виды банковских операций».

Ответственность за принятие решения о введении ограничений и их реализацию возлагается на бизнес-владельца УЦ и подразделение ИБ Банка.

Глава 5. Идентификация и аутентификация владельцев регистрационных свидетельств

§1. Требования к именам

38. УЦ выпускает регистрационные свидетельства, 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. DN содержит персональные данные, которые позволяют однозначно идентифицировать физическое или юридическое лицо — владельца регистрационного свидетельства и определяет владельца регистрационного свидетельства и его закрытого ключа, а также область применения данного сертификата, выданного УЦ.

39. Идентификация владельцев регистрационных свидетельств, являющихся резидентами, достигается за счет использования идентификационных номеров (Индивидуальный идентификационный номер/ Бизнес- идентификационный номер).

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

41. Анонимность владельцев регистрационных свидетельств не допускается.

42. Использование владельцами регистрационных свидетельств псевдонимов вместо собственных имен для физических лиц (фамилии, имени, отчества (при наличии), указанных в документах, удостоверяющих личность физического лица) либо официальных наименований для бизнес-клиентов не допускается.

43. Заявители не должны указывать в заявлениях на выпуск регистрационного свидетельства наименования или иные обозначения, нарушающие права третьих лиц.

44. Центр регистрации может отклонить любое заявление на выпуск регистрационного свидетельства, если при проверке станет известно о факте предоставления недостоверной информации.

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

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

Атрибут	Значение
Country (C=)	KZ
Organization (O=)	Alatau City Bank JSC
Common Name (CN=)	Код владельца регистрационного свидетельства (ФИО/наименование)

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

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

49. В регистрационные свидетельства владельцев в поле «Subject» включается набор

атрибутов, который приведен в нижеследующей таблице:

Атрибут	Значение
Country (C=)	KZ
Organization (O=)	Alatau City Bank JSC
Organization unit (OU=)	Данное поле является не уникальным и в одном регистрационном свидетельстве может быть несколько полей «OU». Одно из значений может соответствовать следующему шаблону: «BIN123456789012». В этом случае длина поля 15 символов. Первые три символа равны «BIN», С 4 по 15 символы только цифры и содержат бизнес идентификационный номер юридического лица.
Common name (CN=)	Код владельца регистрационного свидетельства (ФИО/наименование)
serialNumber	Шаблон поля «IIN123456789012» Длина поля всегда 15 символов, Первые три символа всегда равны «IIN», С 4 по 15 символы только цифры и содержат индивидуальный идентификационный номер физического лица.

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

§2. Первоначальная проверка идентичности владельца

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

52. Центр регистрации проводит первоначальную проверку идентичности владельца в соответствии с правовым актом РК по вопросам выдачи, хранения, отзыва регистрационных свидетельств, изданным уполномоченным органом в сфере информатизации (далее – Правовой акт регулятора)[1].

53. Подтверждение принадлежности и действительности открытого ключа ЭЦП, выданного УЦ, осуществляется участником ИОК с использованием ИС при передаче и получении электронных документов между участниками ИОК.

54. При получении электронного документа, содержащего регистрационные свидетельства подписывающей стороны, участник ИОК с использованием ИС осуществляет проверку в соответствии требованиям Правил проверки подлинности электронной цифровой подписи №1187 от 09.12.2015 года на предмет подтверждения принадлежности и действительности открытого ключа ЭЦП путём:

1) проверки регистрационного свидетельства подписывающей стороны;
2) проверки ЭЦП в электронном документе.

Техническая реализация проверки подлинности ЭЦП и регистрационного свидетельства возлагается на информационную систему.

Глава 6. Операционные требования к жизненному циклу регистрационных свидетельств

§1. Заявления на выпуск (выдачу) регистрационного свидетельства

55. Центр регистрации принимает электронное заявление на выпуск регистрационного свидетельства от клиентов Банка-физических лиц и бизнес-клиентов.

56. Заявление на выпуск (выдачу) регистрационного свидетельства подаётся

[1] Правила выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром, за исключением корневого удостоверяющего центра Республики и развитию Республики Казахстан от 23 декабря 2015 года № 1231.

заявителем в центр регистрации согласно Приложениям 3, 4. Заявителем может быть как владелец, так и доверенное лицо, действующее на основании надлежащим образом оформленных полномочий.

57. Выдача регистрационного свидетельства владельцу осуществляется центром регистрации.

58. Регистрационное свидетельство владельца, выдаваемое УЦ и регистрационное свидетельство УЦ должны соответствовать требованиям м X.509 ITU-T версии 3 и RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile». Сертификат содержит отличительное DN имя в формате, рекомендуемом стандартами X.501 ITU-T в поле «Subject». DN имя сертификата содержит персональные данные, позволяющие идентифицировать физическое или юридическое лицо подписчика УЦ. DN имя определяет владельца сертификата и соответствующего закрытого ключа, а также область применения сертификата УЦ.

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

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

61. Заявление на выпуск регистрационного свидетельства содержит указание адреса размещения Политики и Регламента.

62. Заявление на выпуск регистрационного свидетельства является документом, подтверждающим принятие заявителем обязательств владельца регистрационных свидетельств (владельца и доверяющей стороны) соблюдать принципы и выполнять требования Политики и Регламента.

63. Обязательства владельца (в том числе, его представителя) изложены в параграфе 4 главы 11 Регламента («Гарантии и заверения»).

§2. Обработка заявлений на выпуск регистрационных свидетельств

64. В процессе запроса на выдачу регистрационного свидетельства заявитель должен:

1) дать согласие на сбор и обработку персональных данных;

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

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

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

66. Центр регистрации отказывает в приеме электронных документов не позднее дня проведения идентификации и аутентификации заявителя в случае, если заявитель при подаче заявления не прошел успешно процедуру идентификации и аутентификации.

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

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

1) заявитель указал в нем не всю информацию, необходимую в соответствии с требованиями законодательства РК;

2) заявитель указал в нем недостоверные сведения;

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

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

5) в иных случаях, установленных законодательством РК.

69. В случае изменения, определенного законодательством РК перечня оснований для отказа в выдаче регистрационного свидетельства, применяются требования действующего

законодательства РК. Регламент подлежит приведению в установленном порядке в соответствие действующему законодательству РК.

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

§3. Выпуск регистрационного свидетельства

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

1) идентификацию личности заявителя;

2) защищенную генерацию ключевой пары в центре сертификации;

3) защищенную доставку открытого ключа ЭЦП заявителю;

4) проверку факта владения закрытым ключом ЭЦП, соответствующим открытому ключу ЭЦП, который подлежит регистрации УЦ.

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

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

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

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

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

§4. Использование регистрационного свидетельства и ключевых пар

77. Заявитель, действующий на основании регистрационного свидетельства, выпущенного УЦ Банка, осуществляет проверку его действительности с использованием предусмотренных механизмов: OCSP, меток времени, ответов служб CORC и иных доступных подтверждений.

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

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

80. Закрытый ключ ЭЦП используется владельцем только в соответствии с Законом РК «Об электронном документе и электронной цифровой подписи», нормативно правовыми актами РК, а также договорными обязательствами с клиентами Банка, ВД Банка.

81. Проверка ЭЦП осуществляется в обратном порядке, по которому производилась подпись документа, по следующей схеме:

1) с помощью открытого ключа ЭЦП владельца дешифруется хэш сообщения (подпись владельца);

2) с помощью хэш-функции вычисляется контрольная сумма оригинального сообщения.

На данном этапе производится сверка двух контрольных сумм, если они равны, то ЭЦП

владельца считается верной (определен положительный результат проверки ЭЦП), если не равны, то ЭЦП считается не действительной (определен отрицательный результат проверки ЭЦП).

82. ИС Банка в случае, если определен положительный результат проверки ЭЦП проверяет регистрационные свидетельства владельца путем выполнения следующих проверок с использованием СКЗИ и средств ЭЦП УЦ:

1) проверка срока действия регистрационного свидетельства. Проверка сроков действия от регистрационного свидетельства владельца до доверенного корневого регистрационного свидетельства удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;

2) проверка регистрационного свидетельства на отозванность (аннулирование). Проверка регистрационного свидетельства на отозванность (аннулирование) осуществляется одним из следующих методов:

- на основе СОРС УЦ. Данный метод проверки подтверждает, аннулировано ли проверяемое регистрационное свидетельство на момент начала срока действия СОРС УЦ;
- онлайн проверка регистрационного свидетельства на аннулирование, основанная на протоколе On-line Certificate Status Protocol (далее - OCSP). Данный метод проверки подтверждает аннулировано ли проверяемое регистрационное свидетельство на момент формирования квитанции OCSP;
- на основе дополнительного СОРС. Данный сервис используется совместно с сервисом СОРС. Данный метод проверки подтверждает, аннулировано ли проверяемое регистрационное свидетельство на момент начала срока действия дополнительного СОРС УЦ;

3) проверка области использования ЭЦП регистрационного свидетельства. Проверка заключается в проверке значения поля регистрационного свидетельства «использование ключа» (KeyUsage). Значения «Цифровая подпись» и «Неотрекаемость», содержащиеся в поле «использование ключа», означают что, это регистрационное свидетельство используется для ЭЦП. Значения «Цифровая подпись» и «Шифрование ключей», содержащиеся в поле «использование ключа», означают что, это регистрационное свидетельство используется для аутентификации;

4) проверка номера политики регистрационного свидетельства и разрешенных способах его использования. Политика проверяемого регистрационного свидетельства содержит разрешенные и запрещенные способы использования регистрационного свидетельства, это означает, что данное регистрационное свидетельство не может использоваться в других ИС;

5) проверка построения корректной цепочки от проверяемого регистрационного свидетельства до доверенного корневого регистрационного свидетельства удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;

6) проверка метки времени. Проверка квитанции метки времени осуществляется для электронных документов долговременного хранения. Квитанция метки времени формируется в момент подписания электронного документа при определении положительного результата проверки ЭЦП, тем самым являясь доказательством подписания документа в указанный момент времени.

Метка времени является доказательством наличия ЭЦП в указанный в квитанции момент времени;

7) проверка полномочий лица, подписавшего документ. Механизмы проверки полномочий осуществляются ИС Банка. Проверка полномочий осуществляется при наличии информации об этом в регистрационном свидетельстве.

83. Если один из шагов проверки дает отрицательный результат или его невозможно выполнить, то ЭЦП считается недействительной и ИС Банка отклоняет электронный документ.

§5. Смена ключей в регистрационном свидетельстве

84. Для смены ключей и дальнейшего использования сервисов центра сертификации, требующих наличия ключей, владелец регистрационного свидетельства повторно проходит процедуру выпуска (нового) регистрационного свидетельства в порядке, определенным Регламентом.

85. Смена ключей – подразумевает выпуск нового закрытого ключа ЭЦП и соответствующего ему регистрационного свидетельства с открытым ключом ЭЦП. Процедура подачи заявления и выдачи регистрационного свидетельства при смене ключей полностью аналогична процедурам подачи заявления на выпуск (выдачу) регистрационного свидетельства и его обработки.

86. Замена ключей до истечения срока действия регистрационного свидетельства может быть выполнена при предоставлении через центр регистрации заявления на перевыпуск ключей ЭЦП (выдачу нового регистрационного свидетельства), подписанного закрытым ключом ЭЦП, который соответствует действующему регистрационному свидетельству владельца.

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

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

§6. Изменение данных в регистрационном свидетельстве

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

90. Для изменения данных в регистрационном свидетельстве его владелец повторно проходит процедуру выпуска (нового) регистрационного свидетельства в порядке, определенным Регламентом.

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

§7. Отзыв регистрационных свидетельств

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

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

94. Для отзыва регистрационного свидетельства владелец регистрационного свидетельства через центр регистрации подает заявление на отзыв регистрационного свидетельства по форме, согласно Приложениям 5, 6 к настоящему Регламенту.

95. УЦ отзывает регистрационное свидетельство в следующих случаях:

1) по требованию владельца регистрационного свидетельства;

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

3) смерти владельца регистрационного свидетельства;

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

5) смены наименования, реорганизации, ликвидации юридического лица - владельца регистрационного свидетельства, смены руководителя юридического лица;

6) предусмотренных соглашениями/договорами, заключенных между Банком и заявителем;

7) по вступившему в законную силу решению суда.

УЦ производит отзыв регистрационного свидетельства без заявления от владельца (его

законного представителя) при наступлении одного из случаев, указанных в настоящем пункте, за исключением подпункта 1) настоящего пункта.

96. Отзыв регистрационного свидетельства по требованию владельца регистрационного свидетельства осуществляется в течение 1 (одного) рабочего дня.

97. В случае изменения, определенного законодательством РК перечня оснований для отзыва регистрационного свидетельства, применяются требования действующего законодательства РК.

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

99. Перед отзывом регистрационного свидетельства в случаях, указанных в подпунктах 1) и 4) пункта 94, заявитель проходит идентификацию и аутентификацию в центре регистрации.

100.Процедура отзыва регистрационного свидетельства осуществляется в соответствии с Правовым актом регулятора и настоящей главой Регламента.

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

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

1) публикует в хранилище обновляемые СОРС согласно параграфу 1 Главы 4 Регламента;

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

103.УЦ не предоставляет услуги по временному приостановлению или возобновлению действия регистрационного свидетельства.

104.УЦ не осуществляет хранение (депонирование) закрытого ключа ЭЦП владельца регистрационного свидетельства, за исключением случаев, предусмотренных законодательством РК, связанных с использованием облачной ЭЦП, когда закрытый ключ ЭЦП хранится в модуле безопасности (HSM) УЦ на основании согласия заявителя.

105.Актуальный СОРС УЦ доступен в официальном сайте Банка круглосуточно и непрерывно, за исключением времени плановых профилактических работ в соответствии с условиями соглашения об уровне обслуживания УЦ.

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

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

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

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

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

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

110.В случае компрометации закрытых ключей УЦ Администратор УЦ незамедлительно уведомляет по корпоративной электронной почте бизнес-владельца УЦ Банка, использующего сервисы центра сертификации и центра регистрации. Бизнес-владелец УЦ совместно с ответственными подразделениями Банка принимает меры по приостановке

использования скомпрометированных регистрационных свидетельств, минимизации рисков посредством публикации информации на сайте Банка, уведомления владельцев регистрационных свидетельств и организации выдачи новых регистрационных свидетельств владельцам скомпрометированных регистрационных свидетельств. По завершении мероприятий предоставляется отчет о принятых мерах и результатах расследования.

Глава 7. Виды контроля Удостоверяющего центра

§1. Физический контроль

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

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

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

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

3) ВД, регламентирующим порядок монтажа и размещения систем видеонаблюдения.

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

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

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

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

117.Выделенные к уничтожению документы, не подлежащих архивному хранению, и их уничтожение осуществляется работниками УЦ, обеспечивающими документирование. Сменные носители информации перед утилизацией подлежат физическому уничтожению методами механического разрушения (измельчение, перфорация, раздавливание), термического уничтожения (сжигание), демагнетизации (воздействие сильного магнитного поля), химического разложения или шредирования (дробление на мелкие частицы), исключающими возможность восстановления данных.

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

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

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

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

4) ВД, регламентирующим порядок технического оснащения серверных помещений.

119.Центр сертификации обеспечен 2 (двумя) центрами обработки данных (основной и

резервный), расположенными на разных объектах, в целях резервирования и восстановления функционирования в случае чрезвычайной ситуации, согласно ПП НБРК № 34 «Об утверждении Требований к безопасности и беспрерывности работы информационных систем банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций».

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

121.Серверные помещения центров обработки оборудованы системами:

1) контроля и управления доступом;
2) охранной сигнализации;
3) видеонаблюдения;
4) гарантированного электропитания;
5) электрического заземления;
6) обеспечения микроклимата;
7) пожарной сигнализации;
8) газового автоматического пожаротушения.

122.Независимость подразделений, реализующих меры пропускного и внутриобъектового режима в Банке, от центра сертификации обеспечиваются разграничением их функций, подчиненности и зон ответственности, исключающим возможность административного или функционального влияния центра сертификации на деятельность данных подразделений, а также отсутствием пересечения в процессах принятия решений, контроля и отчетности. Контроль процессов, реализующих меры пропускного и внутриобъектового режима в Банке, обеспечивается подразделением безопасности в соответствии с ВД, регламентирующим процедуру организации пропускного и внутриобъектного режимов в Банке и службой внутреннего аудита посредством независимой оценки в соответствии с ВД Банка, регламентирующим процедуру эффективности системы внутреннего контроля, системы управления рисками, корпоративного управления по всем направлениям деятельности Банка

.

§2. Операционный контроль

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

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

1) доступность сервисов – 99,5% в режиме 24/7/365, то есть не более 1 (одних) суток 19 (девятнадцати) часов и 50 (пятьдесят) минут простоя в год, без учета плановых работ;
2) скорость обработки запросов каждого типа – не ниже 8 (восьми) запросов в минуту;
3) обслуживание не менее 4 000 000 (четырех миллионов) регистрационных свидетельств в операционном доступе.

125.Допустимое время простоя оборудования в центрах обработки данных по причине отказов оборудования и каналов связи составляет не более 18 (восемнадцати) часов в год, что составляет 99.8% (девяносто девять тысяч восемь десятых процентов). За исключением плановых работ по модернизации и/или форс-мажорных обстоятельств, неподконтрольных поставщикам услуг. Данные условия фиксируются к соглашениям об уровне обслуживания (SLA), заключаемых между банком и поставщикам услуг.

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

127.Требования, указанные в пунктах 129-132, должны быть закреплены в качестве обязательств поставщиков услуг в договорах, заключаемых Банком с соответствующими поставщиками услуг

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

129. Все операции с устройствами HSM, включая использование ключей для физического доступа и ключей активации, осуществляются при обязательном участии не менее 2 (двух) уполномоченных работников Банка из подразделения ИБ и подразделения технического сопровождения HSM, назначенных в соответствии с ВД, регулирующими распределение ролей и полномочий.

130.Работники, осуществляющие операционный контроль за работой HSM (например, администратор УЦ, системный администратор УЦ), не имеют доступа к ключевому материалу и не выполняют операций с ним. В свою очередь, работники, участвующие в управлении ключевым материалом (генерация, импорт, загрузка в HSM и т.д.), не осуществляют операционный контроль и не выполняют администрирование устройств HSM. Разделение ролей устанавливается в целях обеспечения безопасности и исключения конфликта интересов.

§3. Управляющий контроль

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

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

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

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

§4. Процедуры контрольного протоколирования

135. УЦ обеспечивает протоколирование следующих событий:

1) формирование закрытого ключа ЭЦП облачной ЭЦП;
2) использование закрытого ключа ЭЦП облачной ЭЦП;
3) 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:

1) идентификатор владельца;
2) дата и время;
3) событие.

136.Протоколы событий ежедневно преобразуется в хэш, и данные хэш хранятся в цепочке событий блокчейн. Применяемый для этого блокчейн доступен на официальном сайте Банка. Публикация хэша на официальный сайт Банка осуществляется для обеспечения неизменности и проверки целостности событий, а также для возможности независимой верификации данных.

137.В УЦ обязательному протоколированию подлежат следующие типы событий:

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

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

регистрационных свидетельств, генерация и выпуск CORC);

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

4) жизненный цикл заявлений на выпуск и отзыв регистрационных свидетельств (данные идентификации и аутентификации, дата и время обработки);

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

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

139.Контрольные протоколы УЦ подлежат ежедневному резервному копированию, ежемесячному архивированию с регистрацией, передаче бизнес-владельцем УЦ в архив и хранению в течение 1 (одного) года с обеспечением доступа и восстановления.

140.Документы (заявления и иные подтверждающие документы) владельцев регистрационных свидетельств и контрагентов УЦ регистрируются, систематизируются и хранятся в соответствии с ВД Банка, регулирующим вопросы делопроизводства.

§5. Смена ключей Удостоверяющего центра

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

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

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

144.Заблаговременно, до окончания срока действия закрытого ключа ЭЦП уполномоченного лица УЦ, Администратор УЦ производит формирование нового закрытого ключа ЭЦП и регистрационного свидетельства уполномоченного лица УЦ и публикует его в соответствующий раздел хранилища. По окончании действия закрытого ключа ЭЦП, носители ключевой информации с закрытым ключом ЭЦП и его копиями уничтожаются по акту, в соответствии с ВД Банка, регламентирующим уничтожение электронной информации и (или) неисправных электронных носителей информации. Все владельцы регистрационных свидетельств обязаны получить новое регистрационное свидетельство УЦ и добавить его в справочники регистрационных свидетельств без удаления действующего регистрационного свидетельства УЦ.

§6. Восстановление функционирования в случае чрезвычайных происшествий или компрометации

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

146.В Инструкции во внештатных, кризисных ситуациях, Инструкции по резервному копированию и в Правилах по обеспечению непрерывной работы активов предусмотрены:

1) переключение для восстановления функционирования УЦ на рабочий центр обработки данных;

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

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

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

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

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

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

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

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

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

152. Обоснованные подозрения в компрометации закрытых ключей УЦ обрабатываются как инцидент информационной безопасности критического уровня и подлежат немедленному расследованию уполномоченным подразделением информационной безопасности Банка в соответствии с ВД Банка, регламентирующим управление инцидентами информационной безопасности.

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

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

§7. Ведение архива

155.УЦ ведет архив в электронном формате:

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

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

3) контрольных протоколов информационной системы.

156.Хранение носителей архивной информации, маркировка архивных носителей информации, защита данных архива от несанкционированного просмотра, изменения и удаления осуществляются в соответствии с Инструкцией по эксплуатации магнитных лент

системы резервного копирования и жестких дисков серверного оборудования и систем хранения данных.

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

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

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

160.Внешнее резервирование архива центра сертификации не предусматривается.

Глава 8. Технический контроль безопасности

§1. Генерация и установка ключей

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

162.Доступ работников или центра регистрации к закрытым ключам ЭЦП владельцев регистрационных свидетельств технически исключен за счет использования исключительно защищенных носителей ключевой информации (аппаратных криптографических модулей HSM, USB-токенов, смарт-карт и иных сертификационных устройств, обеспечивающих невозможность извлечения закрытого ключа ЭЦП в открытом виде).

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

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

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

166.Открытые ключи УЦ (в составе регистрационных свидетельств) также доступны для загрузки с официального сайте Банка.

167.УЦ выдает ключи, предназначенные для использования в соответствии с международным стандартом СТ РК ГОСТ Р 34.10-2015 (ЭЦП):

Длина закрытого ключа ЭЦП – 256 двоичных разрядов.

Длина открытого ключа ЭЦП – 512 двоичных разрядов.

168.Закрытые ключи ЭЦП создаются УЦ в облачной ЭЦП.

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

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

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

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

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

170.В центре сертификации закрытые ключи ЭЦП владельцев генерируются непосредственно на защищенном носителе ключевой информации (HSM), исключающем

возможность его разглашения, изменения или несанкционированного использования.

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

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

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

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

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

176.При выгрузке резервной копии закрытых ключей УЦ из аппаратного криптографического модуля (HSM) создается секрет (данные активации), который делится на n частей. Для активации ключей после их восстановления из резервной копии достаточно задействования m частей секрета при участии их хранителей. Текущее значение параметров m из n зафиксировано в паспорте HSM (на момент издания настоящего Регламента n = 5 и m = 3). Резервная копия закрытого ключа Центра Сертификации хранится отдельно от криптографического модуля в зашифрованном архиве.

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

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

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

180.На этапе хранения резервная копия закрытых ключей УЦ защищена от разглашения, искажения и подмены криптографическими (шифрование, контроль целостности) и организационными (ограничение доступа, разграничение полномочий, ведение журналов) мерами.

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

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

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

§3. Иные аспекты управления ключами

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

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

186.Срок действия регистрационных свидетельств владельцев, поступившие через центр регистрации, составляют 1 (один) год и устанавливается нормативно-технической документацией, заинтересованной ИС Банка, в соответствии с параграфом 3 главы 4 Регламента.

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

§4. Данные активации закрытого ключа ЭЦП

188.Для использования закрытого ключа ЭЦП владельцу необходимо создать и применять данные активации в форме пароля.

189.При первичной установке пароля участник ИОК (за исключением владельцев регистрационных свидетельств) обязан произвести его замену сразу после первого подключения к ИС Банка или первичной активации защищенного носителя ключевой информации (USB-токена, смарт-карты, HSM модуля), при этом пароль:

1) не должен быть менее 12 (двенадцать) символов (для администраторов систем – не менее 16 (шестнадцать) символов);

2) сложность пароля – возможность проверки наличия в пароле как минимум трех групп символов: строчных букв, заглавных букв, цифровых значений, специальных символов. Проверка пароля на соответствие данному параметру производится при каждой смене пароля, в случае несоответствия владелец уведомляется.

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

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

2) должен содержать только цифровые значения.

191.Запрещается записывать пароль доступа к ключу. Пароль должен быть известен только владельцу ключа. Запрещается использование функции автоматического сохранения пароля в программных или аппаратных средствах безопасности (USB-токенах, смарт-картах и иных сертифицированных устройствах).

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

193.Каждый хранитель (участник ИОК) части секрета, которая предназначена для активации закрытых ключей УЦ, хранит свой пароль в тайне и несет ответственность за

нарушение данного требования, предусмотренную трудовым договором и должностной инструкцией.

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

§5. Контроль безопасности вычислительных ресурсов

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

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

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

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

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

200.В деятельности центра сертификации используются средства криптографической защиты информации (СКЗИ: HSM и программные СКЗИ), сертифицированные на соответствие требованиям законодательства РК в области информационной безопасности, включая стандарты защиты данных в финансовом секторе, а также международные стандарты безопасности криптографических модулей.

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

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

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

§6. Контроль использования программного обеспечения

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

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

206.В целях апробации любых изменений в центре сертификации бизнес-владелец УЦ создает и поддерживает ее тестовый контур, обеспеченный необходимым минимумом вычислительной техники, средств криптографической защиты информации и лицензий на использование программного обеспечения.

207.Регистрационные свидетельства, СОРС, ответы квитанции (ответы службы) OCSP, контрольные протоколы центра сертификации, содержащие информацию о выпуске и

изменении статуса регистрационных свидетельств, содержат информацию о дате и времени событий.

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

Глава 9. Профили регистрационных свидетельств, СОРС и OCSP

§1. Профили регистрационных свидетельств

209.Регистрационные свидетельства, выпускаемые УЦ, соответствуют рекомендациям RFC 3280 с маркировкой по версии 3 (v.3) – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (профиль сертификатов X.509 версии 3 и списков отзыва сертификата версии 2).

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

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

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

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

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

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

Название	Формат

СТ РК ГОСТ Р 34.10-2015	{iso(1) member-body(2) kz(398) certification-authorities(3) basic-cryptography(10) algorithms(1) digital-signature(1) GOST- 34.10-2015 (2) }

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

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

§2. Профили списка отозванных регистрационных свидетельств

216.СОРС, выпускаемые УЦ, соответствуют рекомендациям RFC 3280 с маркировкой по версии 2 (v.2) – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (профиль сертификатов X.509 версии 3 и списков отзыва сертификата версии 2 (v2)).

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

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

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

Название	Критичность
reasonCode	FALSE
certificateIssuer	FALSE

§3. Профиль сервиса OCSP

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

220.Сервис OCSP для получения информации о статусе регистрационных свидетельств, выпущенных УЦ, предоставляется центром сертификации в формате версии 1 (согласно рекомендациям RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP», онлайн протокол статуса сертификатов интернет-инфраструктуры

открытых ключей ЭЦП X.509).

Глава 10. Проверка деятельности

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

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

Глава 11. Прочие положения

§1. Тарифы

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

1) выпуск регистрационного свидетельства;
2) отзыв регистрационного свидетельства;
3) размещение регистрационных свидетельств и CORC в хранилище;
4) предоставление информации о статусе регистрационных свидетельств в режиме онлайн по протоколу OCSP;
5) привязка данных к реальному времени в режиме онлайн по протоколу TSP (Time stamp protocol – сервис «метки времени»).

§2. Защита персональных данных участников

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

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

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

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

§3. Права интеллектуальной собственности

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

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

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

§4. Гарантии и заверения

231.Центр сертификации обеспечивает:

1) соответствие данных, содержащихся в выпущенных им регистрационных свидетельствах, тем сведениям, которые предоставил центр регистрации в составе запроса на

выпуск регистрационного свидетельства, и отсутствие в данных регистрационных свидетельствах случайных или умышленных искажений этих сведений по умыслу или в результате ошибочных действий работников УЦ;

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

3) публикацию Политики и Регламента на официальном сайте Банка.

232.Центр регистрации обеспечивает:

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

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

233.Каждый владелец регистрационного свидетельства обеспечивает:

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

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

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

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

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

235.Центр сертификации не несет перед владельцами регистрационных свидетельств (доверяющими сторонами) иной ответственности, кроме той ответственности, которая установлена законодательством РК по вопросам электронного документа и ЭЦП и задекларирована Политикой.

§5. Уведомления и связь с участниками

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

§6. Разрешение споров

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

238.Для разрешения споров, предметом которых являются разногласия по существу настоящего Регламента, применяется законодательство РК.

239.В случае наступления обстоятельств непреодолимой силы (форс-мажор) Банк и владельцы регистрационных свидетельств – руководствуются соответствующими положениями действующих между ними договоров (при наличии).

Глава 12. Ответственность

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

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

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

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

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

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

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

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

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

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

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

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

245.Ответственность за надлежащее исполнение Регламента возлагается на работников и руководителей УЦ, указанных в пункте 244 Регламента.

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

247.Руководители и работники УЦ, указанных в пункте 244 Регламента, участвующие в деятельности УЦ несут ответственность за организацию и осуществление внутреннего контроля в соответствии с положениями ВД Банка, регламентирующих политику внутреннего контроля и процедуру осуществления внутреннего контроля в Банке.

248.Руководители и работники УЦ, указанные в пункте 244 Регламента, участвующие в деятельности УЦ, обязаны строго придерживаться принципа недопущения конфликта интересов при исполнении своих функциональных обязанностей и несут ответственность за соблюдение положений ВД Банка, регламентирующих политику управления конфликтами интересов в Банке. В случае возникновения конфликта интересов руководители и работники УЦ, оповещают об этом непосредственного руководителя и подразделение по управлению комплаенс-риском.

Глава 13. Заключительные положения

249.Регламент 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) со дня утверждения Правлением, если решением Правления не установлен иной срок введения его в действие.

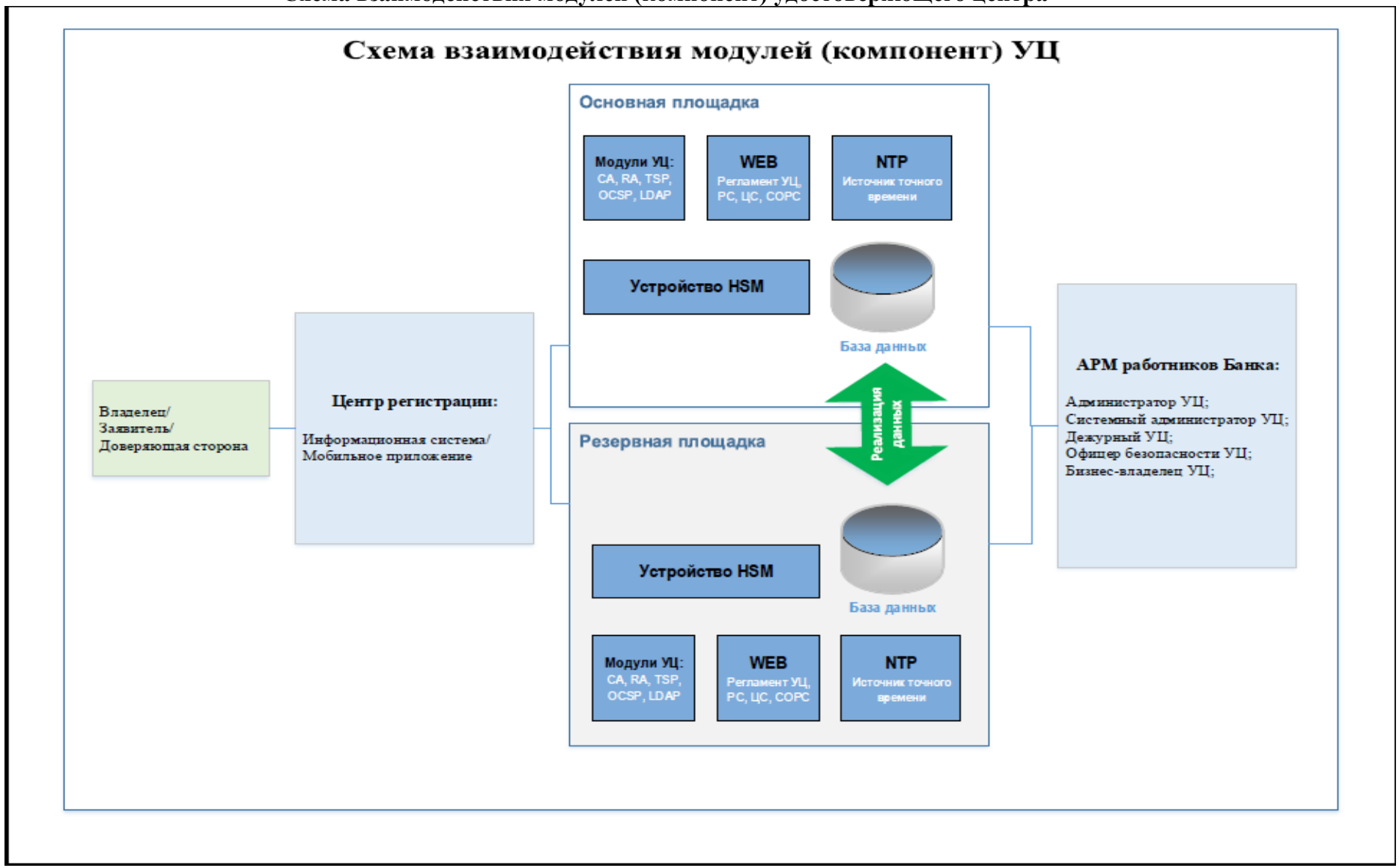
250.Решение о признании утраты силы Регламента вступает в силу в день ввода в действие новой редакции Регламента или замещающего его внутреннего документа или по истечении 10 (десяти) рабочих дней со дня принятия решения Правлением, если не установлен иной срок решением Правления.

251.Положения, не урегулированные Регламентом, регулируются законодательством Республики Казахстан и внутренними документами Банка.

252.В случае изменения законодательства Республики Казахстан и возникновения противоречий отдельных положений Регламента законодательству Республики Казахстан, такие положения Регламента утрачивают силу, и работники Банка руководствуются в своей деятельности законодательством Республики Казахстан до соответствующей актуализации и/или внесения изменений в Регламент.

Приложение 1
к Регламенту деятельности Удостоверяющего центра АО «Alatau City Bank»

Схема взаимодействия модулей (компонент) удостоверяющего центра



ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к Схеме взаимодействия модулей (компонент) Удостоверяющего центра

Взаимодействие компонентов (основной и резервный центр)

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

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

Безопасность взаимодействия модулей УЦ обеспечивается использованием сертифицированного средства криптографической защиты информации «TUMAP-CSP», соответствующего 2 (второму) уровню безопасности согласно СТ РК 1073-2007.

Для хранения и обеспечения безопасности закрытых ключей УЦ используются защищенные программно-аппаратные комплексы HSM, соответствующие 2 (второму) и 3 (третьему) уровням безопасности согласно СТ РК 1073-2007.

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

Взаимодействие между рабочим и резервным серверами центров обработки данных

Хранение и управление данными обеспечивается СУБД PostgreSQL.

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

Защита реплицируемых данных обеспечивается шифрованием с применением протокола TLS.

Взаимодействие владельцев с Удостоверяющим центром

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

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

Взаимодействие работников УЦ с модулями Удостоверяющего центра

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

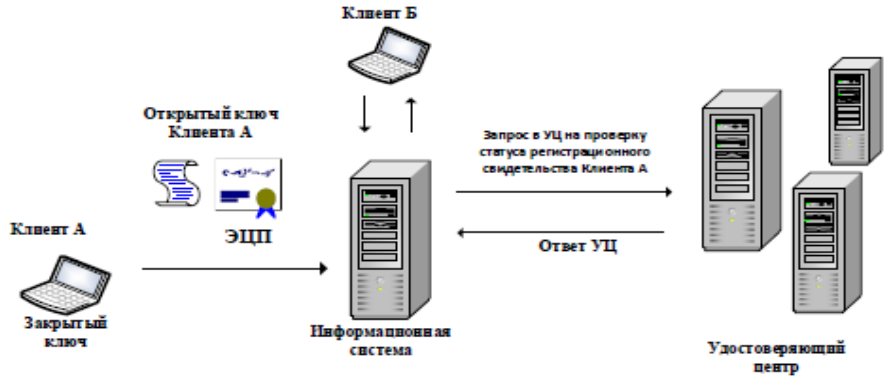
Доступ с рабочего места вышеуказанного работника УЦ к модулям центра сертификации возможен только при наличии действующего регистрационного свидетельства с определенными свойствами.

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

Приложение 2
к Регламенту деятельности Удостоверяющего центра АО «Alatau City Bank»

Схемы ЭЦП с данными о применяемых алгоритмах криптографических преобразований и другими исходными данными (основными требованиями) по реализации процесса формирования ЭЦП и требованиями к отдельным параметрам и Удостоверяющему центру.

Схема электронной цифровой подписи

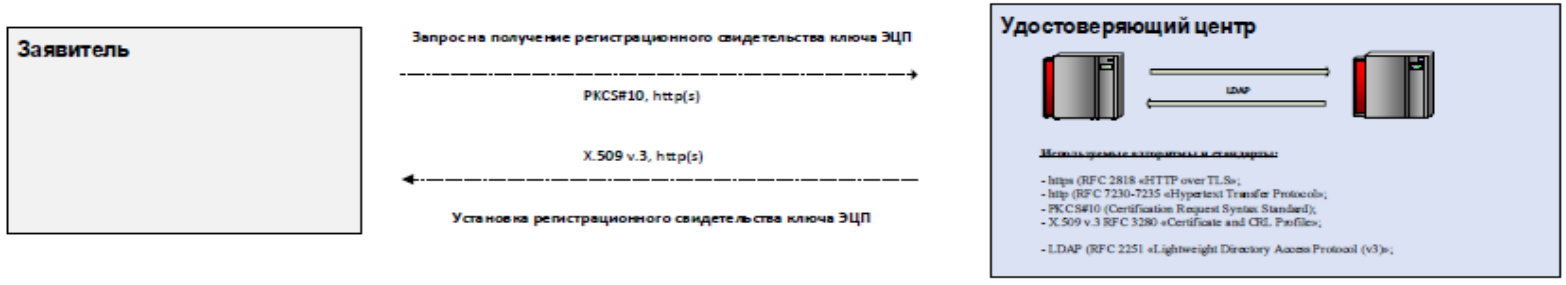


Используемые алгоритмы и стандарты:

ГОСТ Р 34.10-2015 «Информационная технология Криптографическая защита информации Процессы формирования и проверки электронной цифровой подписи

ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хеширования.

Схема взаимодействия клиента и УЦ



Приложение 3
к Регламенту деятельности Удостоверяющего центра АО «Alatau City Bank»

Жеке тұлғадан тіркеу куәлігін беруге өтініш[1]	**Заявление на выдачу регистрационного свидетельства от физического лица[1]**
1. Тіркеу куәлігінің нөмірі*:* _____	1. Номер регистрационного свидетельства*:* _____
2. Жеке сәйкестендіру нөмірі *: _____	2. Индивидуальный идентификационный номер*: _____
3. Резидент еместер үшін - жеке басын куәландыратын құжаттың нөмірі, оның берілген күні, берілген мемлекеті көрсетілген берген органның атауы немесе бірегей нөмірі) *: - _____	3. Для нерезидентов - номер документа, удостоверяющего личность, дата его выдачи, наименование выдавшего органа с указанием государства выдачи или уникальный номер) *: - _____
4. Тегі**:* _____	4. Фамилия**:* _____
5. Аты*: _____	5. Имя*: _____
6. Әкесінің аты: _____	6. Отчество: _____
7. Тіркелген/тұрғылықты мекенжайы *(облыс, қала, көше және т. б. форматында):* _____	7. Адрес прописки/проживания *(в формате области, города, улицы и т.д.):* _____
8. Электрондық пошта мекенжайы*:* _____	8. Адрес электронной почты: _____
9. Телефон: ___ _____	9. Телефон: _____
10. Тіркеу куәліктерінің жарамдылық мерзімі: _____	10. Срок действия регистрационного свидетельства: _____
11. Электрондық цифрлық қолтаңбаны қолдану және қолдануды шектеу салалары туралы ақпарат: «*Alatau City Bank» АҚ банк өнімдері/қызметтері бойынша шарттарға/өтініштерге, сондай-ақ «Alatau City Bank» АҚ қашықтан қызмет көрсету жүйелерінде көзделген өзге де құжаттарға қол қою үшін*.	11. Информацию о сферах применения и ограничениях применения электронной цифровой подписи: *для подписания договоров/заявлений по банковским продуктам/услугам АО «Alatau City Bank», а также иных документов, предусмотренных системами удаленного обслуживания АО «Alatau City Bank».*
12. ЭЦҚ ашық кілті: _____	12. Открытый ключ ЭЦП: _____
13. Қосымша ақпаратқа арналған орын: _____	13. Место для дополнительной информации: _____
14. *Осымен мен* _____ *(ТАӘ толық көрсетіледі)* *растаймын:* • *Мен ұсынған жоғарыда көрсетілген мәліметтер сенімді болып табылады.* • *«Alatau City Bank» АҚ Куәландыру орталығының Тіркеу куәліктерін қолдану саясатымен және «Alatau City Bank» АҚ куәландыру орталығы қызметінің регламентімен (https://alataucitybank.kz) таныстым. Тіркеу куәліктері иесінің*	14. Настоящим *я,* _____ *(указывается ФИО полностью)* *подтверждаю, что:* • *Предоставленные мною вышеуказанные сведения являются достоверными.* • *С Политикой применения регистрационных свидетельств Удостоверяющего центра АО «Alatau City Bank» и Регламентом деятельности Удостоверяющего центра АО «Alatau City Bank» (https://alataucitybank.kz) ознакомлен. Обязуюсь выполнять требования*

[1] Жеке тұлғаларға – дара кәсіпкерлер (шаруа (фермер) қожалықтары) немесе Қазақстан Республикасының заңнамасында белгіленген тәртіппен жеке практикамен айналысатын адамдар (жеке нотариустар, жеке сот орындаушылары, адвокаттар және кәсіби медиаторлар), қаржы басқарушылары жатады

[1] К физическим лицам также относятся 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

* обязательные к заполнению поля/міндетті түрде толықтырылатын өрістер

кепілдіктері мен куәліктерін қоса алғанда, көрсетілген құжаттардағы талаптарын орындауға міндеттенемін. • *Электрондық цифрлық қолтаңбаны (бұдан әрі – ЭЦҚ) алу мақсатында Жеке тұлғадан тіркеу куәліктерін беруге осы өтінішке қол қою арқылы «Alatau City Bank» АҚ-қа, БСН 920140000084 (бұдан әрі – Банк):* *1)Банктің, Банктің үлестес тұлғаларының, банкке қызмет көрсететін үшінші тұлғалардың менің дербес деректерімді жинауына, өңдеуіне, оның ішінде оларды трансшекаралық беруіне, деректерді өңдеудің кез келген қолжетімді технологияларын қолдануына, мені және менің құжаттарымды суретке түсіруіне;* *2)Банктің мен, оның ішінде жаңартулар туралы ақпаратты жинақтаушы зейнетақы қорларынан және «Азаматтарға арналған үкімет «мемлекеттік корпорациясы» КЕАҚ-тан, сондай-ақ мемлекеттік органдардың, басқа ұйымдар мен тұлғалардың дерекқорларынан тікелей және үшінші тұлғалар арқылы кез келген өзге де ақпаратты алуына келісемін;* • *Мен дұрыс емес мәліметтерді ұсынған жағдайда, оның ішінде биометриялық сәйкестендіруден өтпеген және ЭЦҚ жабық кілті үшін құпиясөз жасалмаған жағдайда, Куәландырушы орталық құжаттарды қабылдаудан және тіркеу куәлігін шығарудан бас тартатынына келісемін;* • *ЭЦҚ жабық кілтін «Alatau City Bank» АҚ куәландырушы орталығының HSM қауіпсіздік модулінде сақтауына келісемін;* • *Менің атыма тіркеу куәлігін беруге тыйым салатын заңды күшіне енген сот шешімі жоқ. (тіркеу куәліктерін шығаруға арналған барлық өтініштерде автоматты түрде толтырылады);* • *Өз құпия сөзімді құпиялықта сақтауға және осы талапты бұзғаным үшін жауапты болуға міндетті боламын.* 15. Дербес және өзге де деректерді жинауға және өңдеуге келісім қолданылады және оны «Alatau City Bank» АҚ-пен кез келген қатынастардың қолданылу мерзімі ішінде жеке тұлға кері қайтарып ала алмайды. 16. Күні «__» _____ 20__ж. 17. Жеке тұлғаның (жеке тұлға өкілінің) қолы: _____ *(ОТР қол қойылады).*	*указанных документов, включая гарантии и заверения владельца регистрационных свидетельств.* • *Подписанием настоящего Заявления на выдачу регистрационных свидетельств от физического лица в целях получения электронной цифровой подписи (далее – ЭЦП) даю свое согласие АО «Alatau City Bank», БИН 920140000084 (далее – Банк) на:* *1) сбор, обработку Банком, аффилированными лицами Банка, третьими лицами, которые оказывают услуги Банку, моих персональных данных, в том числе их трансграничную передачу, применение любых доступных технологий обработки данных, фотографирование меня и моих документов;* *на получение, в том числе обновлении Банком информации обо мне из накопительных пенсионных фондов и НАО «Государственная корпорация «Правительство для граждан», а также любой иной информации из баз данных государственных органов, других организаций и лиц, напрямую и через третьих лиц;* *2) Согласен, что Удостоверяющий центр отказывает в приеме документов и выпуске регистрационного свидетельства в случае представления мной недостоверных сведений, в том числе если мной не была пройдена биометрическая идентификация и не был создан пароль для закрытого ключа ЭЦП;* • *Согласен на хранение закрытого ключа ЭЦП в модуле безопасности HSM удостоверяющего центра АО «Alatau City Bank»;* • *Отсутствует вступившее в законную силу решение суда, запрещающее выдачу регистрационного свидетельства на мое имя (заполняется автоматически во всех заявлениях на выпуск регистрационных свидетельств);* • *Обязан хранить свой пароль в тайне и нести ответственность за нарушение данного требования.* 15. Согласие на сбор и обработку персональных и иных данных действует и не может быть отозвано физическим лицом в течение срока действия любых отношений с АО «Alatau City Bank». 16. Дата «__» _____ 20__г. 17. Подпись физического лица (представителя физического лица): _____. *(подписывается ОТР)*

Өтініштегі жолдардың болуы мен тәртібін куәландырушы орталық айқындайды.	*Наличие и порядок полей в заявлении определяется удостоверяющим центром*

Приложение 4
к Регламенту деятельности Удостоверяющего центра АО «Alatau City Bank»

Заңды тұлғадан тіркеу куәлігін беруге өтініш[1]	**Заявление на выдачу регистрационного свидетельства от юридического лица**[1]
1. Тіркеу куәлігінің нөмірі: _____	1. Номер регистрационного свидетельства: _____
2. Бизнес сәйкестендіру нөмірі*: _____	2. Бизнес - идентификационный номер*: ___
3. Резидент еместер үшін - тіркелген елі көрсетілген қосылған құн салығын төлеушінің тіркеу нөмірі) *: _____	3. Для нерезидентов - регистрационный номер плательщика налог на добавленную стоимость с указанием страны регистрации: *_____
4. Ұйымның атауы*: _____	4. Наименование организации: *_____
5. Атына тіркеу куәліктері берілетін заңды тұлға қызметкерінің сәйкестендіру деректері: Жеке сәйкестендіру нөмірі: *_____	5. Идентификационные данные сотрудника юридического лица, на имя которого выдается регистрационное свидетельство: Индивидуальный идентификационный номер*: _____
6. Резидент еместер үшін – жеке басты куәландыратын құжаттың нөмірі, берілген күні, мемлекеті көрсетілген құжатты берген органның атауын немесе бірегей нөмірін көрсету: *_____	6. Для нерезидентов - номер документа, удостоверяющего личность, дата его выдачи, наименование выдавшего органа с указанием государства выдачи или уникальный номер *: _____
7. Тегі*: _____	7. Фамилия *: _____
8. Аты*: _____	8. Имя *: _____
9. Әкесінің аты: _____	9. Отчество: _____
10. Тіркелген/тұрғылықты мекенжайы *(облыс, қала, көше және т. б. форматында)*: _____	10. Адрес прописки/проживания *(в формате области, города, улицы и т.д.)*: _____
11. Электрондық пошта мекенжайы: _____	11. Адрес электронной почты: _____
12. Телефон: _____	12. Телефон: _____
13. Тіркеу куәліктерінің қолданыс мерзімі: _____	13. Срок действия регистрационного свидетельства: _____
Электрондық цифрлық қолтаңбаны қолдану және қолдануды шектеу салалары туралы ақпарат: «*Alatau City Bank» АҚ банк өнімдері/қызметтері бойынша шарттарға/өтініштерге, сондай-ақ «Alatau City Bank» АҚ қашықтан қызмет көрсету жүйелерінде көзделген өзге де құжаттарға қол қою үшін.*	Информацию о сферах применения и ограничениях применения электронной цифровой подписи: *для подписания договоров/заявлений по банковским продуктам/услугам АО «Alatau City Bank», а также иных документов, предусмотренных системами удаленного обслуживания АО «Alatau City Bank».*
	14. Данные о средствах электронной цифровой подписи, используемых для создания

[1] Заңды тұлғаларға – заңды тұлға (заңды тұлғаның оқшауланған бөлімшелерін (филиалдары мен өкілдіктерін) қоса алғанда, ұйымдық-құқықтық нысаны мен меншік нысанына қарамастан), заңды тұлға құрмай шетелдік құрылым, шетелдік дипломатиялық және консулдық өкілдіктер жатады.

[1] К юридическим лицам относятся – юридическое лицо (независимо от организационно-правовой формы и формы собственности, включая обособленные подразделения юридического лица (филиалы и представительства), иностранная структура без образования юридического лица, иностранные дипломатические и консульские представительства.

* обязательные к заполнению поля/міндетті түрде толықтырылатын өрістер

14. Электрондық цифрлық қолтаңбаның тиісті жеке кілтін жасау үшін пайдаланылатын электрондық цифрлық қолтаңба құралдары туралы деректер, электрондық цифрлық қолтаңба алгоритмінің стандартын және ЭЦҚ ашық кілтінің ұзындығын белгілеу: _____
15. ЭЦҚ ашық кілті: _____
16. Қосымша ақпаратқа арналған орын*:* _____
17. *Өтініш беруші осы өтінішке қол қоя отырып, «Alatau City Bank» АҚ Куәландырушы орталығының (КО) сайтында орналастырылған «Куәландырушы орталықтың қызмет регламентінің» (бұдан әрі – Регламент) және «Куәландырушы орталықтың тіркеу куәліктерін қолдану саясатының» (бұдан әрі – Саясат) талаптарын қабылдайтынын және оларға келісетіндігін растайды, сондай-ақ КО-ға мекенжайы (https://alataucitybank.kz) бойынша Банктің ресми сайтында орналастырылған Дербес және өзге де деректерді жинау және өңдеу туралы келісімнің нысаны бойынша өз дербес деректерін және басқа да деректерді жинауға, өңдеуге келісімін береді және оның мазмұнымен танысқанын, түсінетінін және қабылдайтынын растайды, сондай-ақ онда көрсетілген өзгерістер және (немесе) толықтырулар енгізу тәртібімен келіседі.*
Өтініш беруші осы өтінішке қол қоя отырып, КО-ның тіркеу куәлігін және ЭЦҚ-ның жабық кілтін бұлтты ЭЦҚ-ға жазу арқылы беруіне өз келісімін білдіреді.
Өтініш беруші КО тіркеу куәлігін Регламентте, Саясатта, Қазақстан Республикасының заңнамасында көзделген жағдайларда біржақты тәртіппен кері қайтарып алуы мүмкін екендігі туралы хабардар етілді.
18. Дербес және өзге де деректерді жинауға және өңдеуге келісім қолданылады және Өтініш беруші «Alatau City Bank» АҚ-пен кез келген қатынастардың қолданылу мерзімі ішінде кері қайтарып ала алмайды.
19. Күні «__» _____ 20__ж.
20. Заңды тұлға қызметкерінің (заңды тұлға өкілінің) қолы: _____

(ОТР қол қойылады).

соответствующего закрытого ключа электронной цифровой подписи, обозначение стандарта алгоритма электронной цифровой подписи и длины открытого ключа ЭЦП*:* _____
15. Открытый ключ ЭЦП: _____
16. Место для дополнительной информации: _____
17. *Подписанием настоящего заявления Заявитель (его уполномоченный представитель) подтверждает и принимает условия «Регламента деятельности удостоверяющего центра» (далее – Регламент) и Политики применения регистрационных свидетельств удостоверяющего центра» (далее – Политика) размещенных на сайте Удостоверяющего центра АО «Alatau City Bank» (далее – УЦ), а также дает УЦ согласие на сбор, обработку своих персональных данных по форме Согласия на сбор и обработку персональных и иных данных, размещенного на официальном сайте Банка по адресу (https://alataucitybank.kz), и подтверждает, что ознакомлен, понимает и принимает содержание, а также соглашается с порядком внесения изменений и (или) дополнений, указанным в нем. Подписанием настоящего заявления Заявитель выражает свое согласие на выдачу УЦ регистрационного свидетельства и закрытого ключа ЭЦП путем их записи (хранения) в облачной ЭЦП. Заявитель уведомлен о том, что регистрационное свидетельство может быть отозвано УЦ в одностороннем порядке в случаях, предусмотренных Регламентом, Политикой, законодательством Республики Казахстан.*
18. Согласие на сбор и обработку персональных и иных данных действует и не может быть отозвано Заявителем в течение срока действия любых отношений с АО «Alatau City Bank».
19. Дата «__» _____ 20__г.
20. Подпись сотрудника юридического лица (представителя юридического лица): _____

(подписывается ОТР)

Наличие и порядок полей в заявлении определяется удостоверяющим центром.

Өтініштегі жолдардың болуы мен тәртібін куәландырушы орталық айқындайды.	

Приложение 5
к Регламенту деятельности Удостоверяющего центра АО «Alatau City Bank»

Жеке тұлғадан тіркеу куәлігін кері қайтарып алуға өтініш[1]	**Заявление на отзыв регистрационного свидетельства от физического лица[1]**
1. Жеке сәйкестендіру нөмірі: ___ 2. Резидент еместер үшін - жеке басты куәландыратын құжаттың нөмірі, берілген күні, мемлекеті көрсетілген құжатты берген органның атауын немесе бірегей нөмірін көрсету: _____ 3. Тегі: _____ 4. Аты: _____ 5. Әкесінің аты: _____ 6. Электрондық пошта мекенжайы: _____ 7. Телефон: _____ 8. Тіркеу куәлігінің сәйкестендіру деректері: Сериялық нөмірі: _____ 9. Күні «__» _____ 20__ж. 10.Жеке тұлғаның (жеке тұлға өкілінің) қолы: _____ (*ОТР қол қойылады)* *Өтініштегі жолдардың болуы мен тәртібін куәландырушы орталық айқындайды*.	1. Индивидуальный идентификационный номер: _____ 2. Для нерезидентов - номер документа, удостоверяющего личность, дата его выдачи, наименование выдавшего органа с указанием государства выдачи или уникальный номер: _____ 3. Фамилия: _____ 4. Имя: _____ 5. Отчество: _____ 6. Адрес электронной почты: _____ 7. Телефон: _____ 8. Идентификационные данные регистрационного свидетельства: Серийный номер*:* _____ 9. Дата «__» _____ 20__ г. 10. Подпись физического лица (представителя физического лица): _____ *(подписывается ОТР).* *Наличие и порядок полей в заявлении определяется удостоверяющим центром*

[1] Жеке тұлғаларға - дара кәсіпкерлер (шаруа (фермер) қожалықтары) немесе Қазақстан Республикасының заңнамасында белгіленген тәртіппен жеке практикамен айналысатын адамдар (жеке нотариустар, жеке сот орындаушылары, адвокаттар және кәсіби медиаторлар), қаржы басқарушылары жатады

[1] К физическим лицам также относятся - 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

Приложение 6
к Регламенту деятельности Удостоверяющего центра АО «Alatau City Bank»

Заңды тұлғадан тіркеу куәлігін қайтарып алуға өтініш	**Заявление на отзыв регистрационного свидетельства от юридического лица**
1. Бизнес сәйкестендіру нөмірі: _____	1. Бизнес-идентификационный номер: _____
2. Резидент еместер үшін - тіркелген елі көрсетілген қосылған құн салығын төлеушінің тіркеу нөмірі: _____	2. Для нерезидентов - регистрационный номер плательщика налог на добавленную стоимость с указанием страны регистрации: _____
3. Ұйымның атауы: _____	3. Наименование организации: _____
4. Атына тіркеу куәліктері берілетін заңды тұлға қызметкерінің сәйкестендіру деректері: _____	4. Идентификационные данные сотрудника юридического лица, на имя которого выдается регистрационные свидетельства: _____
5. Жеке сәйкестендіру нөмірі: _____	5. Индивидуальный идентификационный номер: _____
6. Резидент еместер үшін - жеке басты куәландыратын құжаттың нөмірі, берілген күні, мемлекеті көрсетілген құжатты берген органның атауын немесе бірегей нөмірін көрсету: _____	6. Для нерезидентов - номер документа, удостоверяющего личность, дата его выдачи, наименование выдавшего органа с указанием государства выдачи или уникальный номер: _____
7. Тегі: _____	7. Фамилия: _____
8. Аты: _____	8. Имя: _____
9. Әкесінің аты: _____	9. Отчество: _____
10. Электрондық пошта мекенжайы: _____	10. Адрес электронной почты: _____
11. Телефон: _____	11. Телефон: _____
12. Тіркеу куәлігінің сәйкестендіру деректері: Сериялық нөмірі: _____	12. Идентификационные данные регистрационного свидетельства: Серийный номер: _____
13. Күні «__» _____ 20__ж.	13. Дата «__» _____ 20__ г.
14. Заңды тұлғаның (заңды тұлға өкілінің) қолы: _____ (*ОТР қол қойылады)*	14. Подпись сотрудника юридического лица (представителя юридического лица): _____. *(подписывается ОТР)*
Өтініштегі жолдардың болуы мен тәртібін куәландырушы орталық айқындайды.	*Наличие и порядок полей в заявлении определяется удостоверяющим центром.*