Утверждено
Протоколом Правления
АО «Банк ЦентрКредит»
№ 0513/4 от 13.05. 2024 г.

РЕГЛАМЕНТ ДЕЯТЕЛЬНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА АО «БАНК ЦЕНТРКРЕДИТ»

Версия 2.1

Алматы 2024

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент деятельности удостоверяющего центра АО «Банк ЦентрКредит» (далее – Регламент) разработан в соответствии с требованиями правовых актов Республики Казахстан по вопросам электронного документа и электронной цифровой подписи, в целях обеспечения функционирования удостоверяющего центра АО «Банк ЦентрКредит» (далее – Удостоверяющий центр) и определяет порядок его функционирования.

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

Удостоверяющий центр АО «Банк ЦентрКредит» создан для оказания услуг по выдаче регистрационных свидетельств физическим лицам - клиентам Банка на основании действующего законодательства Республики Казахстан:

1) Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V;

2) Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи» от 7января 2003 года №370;

3) Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V;

4) Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан «Об утверждении Правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре» от 27 октября 2020 года № 405/НҚ;

5) Приказ Министра по инвестициям и развитию Республики Казахстан «Об утверждении Правил проверки подлинности электронной цифровой подписи» от 9 декабря 2015 года № 1187;

6) Приказ Министра по инвестициям и развитию Республики Казахстан от 23 декабря 2015 № 1231 «Об утверждении Правил 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»;

7) СТ РК 1073–2007. Средства криптографической защиты информации. Общие требования.

1.1 Термины и определения

Термин	Определение
Аппаратный криптографический модуль (Hardware Security Module)	Аппаратный криптографический модуль, предназначенный для шифрования информации и управления открытыми и закрытыми ключами ЭЦП
Аутентификация	Подтверждение подлинности физического лица путем определения соответствия предъявленных им реквизитов доступа имеющимся в системе
Банк	АО «Банк ЦентрКредит»
Биометрическая аутентификация	Комплекс мер, идентифицирующих личность на основании физиологических и неизменных биологических признаков
Блокчейн	Информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе данных на базе цепочки взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования;
Владелец регистрационного свидетельства	В контексте регламента физическое лицо, на имя которого выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве
Закрытый ключ электронной цифровой подписи	Последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи
Идентификация	Сравнение предъявленного идентификатора физического лица с перечнем зарегистрированных идентификаторов

Информационная система (ИС)	Организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач
Инфраструктура открытых ключей	Комплекс информационных систем, организационных и технических мероприятий, направленный на управление регистрационными свидетельствами в соответствии с законодательством Республики Казахстан об электронном документе и электронной цифровой подписи
Компрометация ключей электронной цифровой подписи	Нарушение безопасности при хранении и(или) использовании закрытого ключа электронной цифровой подписи, в результате которого возникает вероятность его несанкционированного применения
Корневой удостоверяющий центр Республики Казахстан	Удостоверяющий центр, осуществляющий подтверждение принадлежности и действительности открытых ключей электронной цифровой подписи удостоверяющих центров
Многофакторная аутентификация	Способ проверки подлинности пользователя при помощи комбинации различных параметров, в том числе генерации и ввода паролей или аутентификационных признаков (цифровых сертификатов, токенов, смарт-карт, генераторов одноразовых паролей и средств биометрической идентификации)
Носитель ключевой информации	Специализированный носитель, в котором для защиты хранящихся закрытых ключей электронной цифровой подписи используется средство криптографической защиты информации, имеющее сертификат соответствия требованиям стандарта СТ РК 1073–2007 «Средства криптографической защиты информации. Общие технические требования"
Облачная ЭЦП	Сервис удостоверяющего центра, позволяющий создавать, использовать, хранить и удалять закрытые ключи электронной цифровой подписи в HSM удостоверяющего центра, где доступ к закрытому ключу осуществляется владельцем удалённо посредством не менее двух факторов аутентификации, одним из которых является биометрическая.
Облачный сертификат	Регистрационное свидетельство УЦ, выданное владельцу ключа облачной ЭЦП
Объектный идентификатор (OID)	Уникальный набор цифр, который связан с объектом и однозначно идентифицирует его в мировом адресном пространстве объектов
Открытый ключ электронной цифровой подписи	Последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе
Отозванное регистрационное свидетельство	Регистрационное свидетельство, аннулированное в порядке, который установлен правовым актом по вопросам выдачи, хранения, отзыва регистрационных свидетельств, изданным уполномоченным органом в сфере информатизации
Подписчик УЦ (подписывающее лицо)	В контексте регламента физическое лицо, правомерно владеющее закрытым ключом электронной цифровой подписи и обладающее правом на ее использование в электронном документе.
Политика применения регистрационных свидетельств	Документ, который определяет порядок и механизмы работы удостоверяющего центра в части управления регистрационными свидетельствами
Приложение ВСС	Мобильные приложения/цифровые платформы Банка, предоставляющие услуги дистанционного банковского обслуживания для физических лиц
Регистрационное свидетельство	Электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом “Об электронном документе и электронной цифровой подписи”
Регламент деятельности удостоверяющего центра	Документ, который определяет порядок организации основной деятельности удостоверяющего центра, осуществляемой в соответствии с политикой применения регистрационных свидетельств, включая реализацию основных процессов удостоверяющего центра

Сертификат	Регистрационное свидетельство
Список отозванных регистрационных свидетельств (сертификатов)	Часть регистра регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва (аннулирования)
Средство криптографической защиты информации	Средство, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами
Удостоверяющий центр (УЦ)	Удостоверяющий центр Банка. Юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства
Хэш	Преобразование массива входных данных произвольной длины в битовую строку фиксированной длины
Электронная цифровая подпись (ЭЦП)	Набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания
Электронный документ	Документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи

1.2 Перечень сокращений

Аббревиатура	Определение
ИОК	Инфраструктура открытых ключей
ЦР	Центр регистрации
СКЗИ	Средство криптографической защиты информации
HSM	Модуль безопасности CERTEX HSM
DN	Distinguished Names
COPC	Список отозванных регистрационных свидетельств
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol
LDAP	Lightweight Directory Access Protocol v3

1.3 Обзор

Настоящий Регламент определяет правила, процедуры и условия предоставления услуг подписчикам УЦ, связанных с жизненным циклом регистрационных свидетельств УЦ. Регламент применим ко всем участникам ИОК Банка, использующим регистрационные свидетельства УЦ.

1.4 Наименование и идентификация документа

Наименование документа: Регламент деятельности Удостоверяющего центра АО «Банк ЦентрКредит».
Объектный идентификатор: 1.2.398.3.24.1.2.1
Версия документа: 2.1
Адрес сервера для публикации Регламента: https://www.bcc.kz/product/pki/?tab=DPP

1.5 Участники ИОК АО «Банк ЦентрКредит»

1.5.1 Центр Сертификации

Центр Сертификации - программно-аппаратный комплекс для выдачи, обслуживания и отзыва сертификатов ключей, действующий в соответствии с утвержденными правилами и сертифицированный по ГОСТ РК 1073–2007.
Центр Сертификации осуществляет следующие функции ИОК:
- обработка запросов на выдачу и отзыв регистрационных свидетельств;
- публикация COPC и промежуточных COPC;
- обработка запросов к службе OCSP на проверку состояния сертификата;
- обработка запросов к службе TSP на формирование метки времени.

Центры Сертификации УЦ Банка:
- Центр сертификации: CN=Certification Authority
- Облачный центр сертификации: CN=CA Cloud

1.5.2 Центр Регистрации

Функцию Центров Регистрации УЦ выполняют информационные системы Банка, ответственные за прием и проверку документов на выпуск или отзыв сертификатов, а также идентификацию и аутентификацию подписчиков.

1.5.3 Хранилище сертификатов

Для получения доступа к сертификатам, службе проверки сертификатов, хранению архивной информации и для других функций Центр Сертификации использует специализированный справочник – хранилище сертификатов и СОРС.

1.5.4 Владелец сертификата

Физическое лицо, на имя которого Центром Сертификации выдан сертификат, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в сертификате.

1.5.5 Доверяющие стороны

Доверяющая сторона – информационная система, использующая полученные в УЦ сведения о сертификате для проверки принадлежности электронной цифровой подписи владельцу сертификата.
Доверяющими сторонами УЦ являются:
- Корневой Удостоверяющий центр Республики Казахстан;
- Физические лица, граждане РК;
- Информационные системы Банка, использующие регистрационные свидетельства Удостоверяющего центра Банка.

1.6 Использование сертификатов

1.6.1 Допустимое использование сертификата

Сертификаты УЦ применимы для следующих целей:
- подписание электронных документов электронной цифровой подписью;
- проверка электронной цифровой подписи;

1.6.2 Ограничения использования сертификата

Способы использования сертификатов УЦ не должны противоречить действующему законодательству Республики Казахстан, а также требованиям настоящего Регламента.

2 ПУБЛИКАЦИЯ И ХРАНЕНИЕ СВЕДЕНИЙ

2.1 Доступность публичной информации

УЦ обеспечивает публикацию и доступность следующей информации на интернет-ресурсах Банка.
Обеспечивается доступность сервисов УЦ из приложения ВСС:
- CA https://bcc-app.bank.corp.centercredit.kz:62305/
- RA https://bcc-app.bank.corp.centercredit.kz:62310/
- OCSP https://bcc-app.bank.corp.centercredit.kz:62301/
- TSP https://bcc-app.bank.corp.centercredit.kz:62302/

Доступны для скачивания и ознакомления:
- Регламент УЦ https://www.bcc.kz/product/pki/?tab=DPP
- Политика применения регистрационных свидетельств УЦ https://www.bcc.kz/product/pki/?tab=DPP
- СОРС https://uc.bcc.kz/cgi/crl

2.2 Публикация хранилища сертификатов

Центр Сертификации публикует для доступа участникам ИОК УЦ хранилище сертификатов и СОРС. Официальным уведомлением участников ИОК УЦ о выпуске сертификата и СОРС является публикация сертификата и СОРС в хранилище сертификатов.

2.3 Время и частота публикаций хранилища сертификата

Выданные сертификаты и СОРС вносятся в хранилище сертификатов и публикуются не позднее даты начала их действия. Период обновления СОРС составляет 7 календарных дней, публикация СОРС производится по мере появления отозванных сертификатов.
Сведения о статусе сертификата публикуются в соответствии с настоящим Регламентом.

2.4 Доступ к хранилищу сертификатов

Доступ к хранилищу сертификатов осуществляется с использованием LDAP RFC 2251. УЦ осуществляет защиту от несанкционированного доступа к хранилищу сертификатов. Сведения, публикуемые на сайте УЦ, предоставляются участникам информационных систем в режиме свободного доступа с правами «только для чтения».

3 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1 Присваивание имён

3.1.1 DN имена

УЦ выдает сертификаты, соответствующие рекомендациям 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 подписчика УЦ. DN имя определяет владельца сертификата и соответствующего закрытого ключа, а также область применения сертификата УЦ.

3.1.2 Персональные данные

Удостоверяющий центр использует правила именования субъектов, призванные обеспечить однозначную идентификацию владельца любого выпущенного регистрационного свидетельства. Однозначность идентификации достигается за счет максимально возможного использования идентификационных номеров из единого республиканского реестра (ИИН), на основании методов идентификации и аутентификации.

3.1.3 Анонимность или использование псевдонимов

Анонимность и использование псевдонимов при формировании DN имен не допускается.

3.1.4 Уникальность имён

Каждому подписчику УЦ должно соответствовать уникальное DN имя.

3.2 Идентификация и аутентификация

3.2.1 Способ доказательства факта владения закрытым ключом

При обработке запроса на выдачу сертификата УЦ проверяет факт обладания закрытым ключом, соответствующим открытому ключу, на который запрашивается регистрационное свидетельство. Способом доказательства владения закрытым ключом является электронный документ в формате PKCS#10. Подписчик УЦ должен обеспечить защиту от неправомерного доступа и использования закрытого ключа.

3.2.2 Идентификация при выпуске облачного сертификата физического лица

Подача заявлений на выпуск облачных сертификатов для физических лиц осуществляется через дистанционный канал (приложение ВСС). В процессе запроса облачного сертификата подписчик УЦ должен:
- дать согласие на сбор и обработку персональных данных (анкета-соглашение);
- ознакомиться с заявлением на выпуск сертификата;
- ознакомиться с Регламентом УЦ и Политикой РС;
- пройти процедуру многофакторной аутентификации, включая биометрическую аутентификацию.

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

3.2.3 Идентификация при отзыве облачного сертификата для физического лица

Подача заявлений на отзыв облачных сертификатов для физических лиц осуществляется через дистанционный канал (приложение ВСС). В процессе отзыва облачного сертификата подписчик УЦ должен:
- пройти процедуру многофакторной аутентификации, включая биометрическую аутентификацию;
- ввести пароль от сертификата с указанием причины отзыва.

4 ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТА

4.1 Заявление на выдачу сертификата

4.1.1 Лица, имеющие право подавать заявления на выпуск сертификатов

Заявление на выдачу сертификата имеют право подавать физические лица, граждане РК.

4.1.2 Процедура и обязательства по регистрации

Регистрация подписчика в УЦ, осуществляется в соответствии с п. 3.2 настоящего Регламента.

4.2 Обработка заявления на выдачу сертификата

4.2.1 Процедура идентификации и аутентификации заявления

Процедуры идентификации и аутентификации осуществляются в порядке, описанном в пункте 3.2.

4.2.2 Выдача или отказ в выдаче сертификата

УЦ выдает сертификат в случае успешного прохождения заявителем процедур идентификации и аутентификации, описанных в пункте 3.2.
В регистрации сертификата может быть отказано в случае:
- заявителем не представлена (либо представлена не полностью) необходимая информация;
- заявителем представлена недостоверная информация.
- недостижение заявителем шестнадцатилетнего возраста.
- в соответствии со вступившим в законную силу решением суда.

4.3 Выдача сертификата

4.3.1 Действия Центра Сертификации при изготовлении сертификата

Запросы на выпуск сертификатов подписываются ЭЦП уполномоченного работника Банка, имеющим права на выпуск сертификатов.
Запросы на выпуск облачных сертификатов принимаются только от информационных систем Банка. Запросы в Центр Сертификации из системы облачной ЭЦП подписываются служебным ключом.

4.4 Признание сертификата

4.4.1 Действия владельца сертификата, означающие признание сертификата

Следующие действия владельца сертификата означают признание сертификата:
- получение сертификата;
- отсутствие у владельца возражений (претензий) по содержанию сертификата;
- использование сертификата.

4.4.2 Публикация сертификата

Центр Сертификации публикует сертификат в хранилище сертификатов в соответствии с настоящим Регламентом. Публикация сертификата происходит сразу после обработки заявления на выпуск РС в УЦ.

4.4.3 Уведомление участника ИОК о выдаче сертификата

Официальным уведомлением пользователей УЦ о выдаче сертификата является его публикация в хранилище сертификатов УЦ и наличие сертификата в приложении ВСС.

4.5 Использование ключей и сертификатов

4.5.1 Использование закрытого ключа подписчиком

Использование владельцем закрытого ключа и сертификата допускается только после признания сертификата. Использование закрытого ключа допустимо только в соответствии с настоящим Регламентом.
Владелец сертификата УЦ обязан принимать меры для защиты принадлежащего ему закрытого ключа ЭЦП от неправомерного доступа и использования в порядке, установленном действующим законодательством Республики Казахстан.

4.5.2 Использование открытого ключа и сертификата подписчиком

Владелец сертификата должен использовать сертификат строго в соответствии с указанными в нем сведениями и настоящим Регламентом. Получение дополнительных сведений и гарантий, помимо сведений, указанных в сертификате, осуществляется участниками УЦ самостоятельно.
Для проверки и принятия решения о доверии к сертификату УЦ, необходимо использовать действующие "Правила проверки подлинности электронной цифровой подписи".

4.6 Обновление сертификата

Обновление сертификата – процедура получения сертификата с новыми сведениями и сроками действия без изменения открытого ключа, указанного в действующем сертификате.
УЦ не выполняет обновления сертификатов подписчиков.
В случае обновления персональных данных подписчика УЦ необходимо отозвать сертификат в соответствии с пунктом 4.9 настоящего Регламента и выпустить новый в соответствии с пунктом 4.2.

4.7 Смена ключей

Смена ключей – процедура выдачи нового сертификата. Данная процедура подразумевает изготовление нового закрытого ключа и соответствующего ему сертификата.
Процедура подачи заявления и выдачи сертификата при смене ключей полностью аналогична процедурам подачи заявления на выдачу сертификата и его обработки.

4.7.1 Основания для замены ключей в сертификате

Ключ и сертификат могут быть заменены подписчиком самостоятельно, если не истек срок действия сертификата.

4.7.2 Обработка запросов на замену ключей в сертификате

Замена ключей до истечения срока действия сертификата может быть выполнена при предоставлении запроса, подписанного личным ключом, который соответствует действующему сертификату подписчика УЦ. При замене ключей в сертификате по истечению срока действия используется процедура идентификации и аутентификации как при первичном получении сертификата.

4.8 Изменение сведений, указанных в сертификате

Процедура подачи заявления и выдачи сертификата при изменении сведений, указанных в сертификате, полностью аналогична процедурам подачи заявления на выдачу сертификата и его обработки.
Для получения нового облачного сертификата при изменении персональных данных подписчика необходимо отозвать действующий сертификат.

4.9 Отзыв и приостановление действия сертификата

4.9.1 Основания для отзыва сертификата

УЦ может отозвать сертификат и опубликовать его в СОРС в следующих случаях:
- по требованию владельца сертификата;
- при установлении факта предоставления недостоверных сведений при получении сертификата;
- смерти владельца сертификата;
- изменения фамилии, имени или отчества владельца сертификата;
- предусмотренных соглашением между УЦ и владельцем сертификата;
- по вступившему в законную силу решению суда.

4.9.2 Лица, уполномоченные подавать заявления на отзыв сертификатов

Заявление на отзыв сертификата может подавать физическое лицо владелец сертификата.

4.9.3 Процедура идентификации и аутентификации заявления

Процедура идентификации владельца при обработке заявки на отзыв сертификата, выполняется с применением биометрической аутентификации и идентификации.

4.9.4 Процедура подачи заявления на отзыв сертификата

Запрос на отзыв сертификата подписывается владельцем и направляется в УЦ через приложение ВСС. Запрос обрабатывается автоматически при соблюдении процедур идентификации и аутентификации.

4.9.5 Срок обработки заявления на отзыв сертификата

Отзыв облачного сертификата через приложение ВСС обрабатывается немедленно.

4.9.6 Требования к осуществлению проверки факта отзыва сертификата

Любой участник ИОК Банка может проверить статус отзыва сертификата. Для проверки можно использовать СОРС или сервис проверки статуса сертификатов OCSP. Информация об адресах СОРС и OCSP, указана в каждом выданном сертификате и настоящем Регламенте. Сервис проверки документов доступен в приложении ВСС и предназначен для получения списка подписанных документов.

4.9.7 Частота выпуска СОРС

СОРС обновляется каждые 7 календарных дней или по мере поступления запросов на смену статуса сертификатов. Отозванные сертификаты с истекшим сроком действия удаляются из СОРС.

4.9.8 Возможность проверки статуса сертификата в режиме онлайн

Информацию о статусе сертификата можно получить по протоколу проверки статуса сертификатов в режиме онлайн используя сервис службы OCSP. Сервис проверки доступен в приложении ВСС.

4.9.9 Срок хранения отозванных сертификатов

Хранение отозванных сертификатов ведется в течение периода работы УЦ.

4.9.10 Особые требования в случае компрометации секретных ключей

В случае обоснованного подозрения о компрометации закрытого ключа владелец соответствующего сертификата выполняет отзыв сертификата согласно пункту 4.9 настоящего Регламента и при необходимости выполняет выпуск нового сертификата.

4.9.11 Условия приостановления действия сертификата

Не предусмотрено.

4.10 Сервис проверки статуса сертификата в режиме онлайн

Информация о статусах сертификатов доступна с использованием CORC и сервиса проверки статуса сертификатов в режиме онлайн.
CORC предоставляется в электронной форме в формате, определенном RFC 5280. Список заверяется ЭЦП Центра Сертификации. Доступ к CORC обеспечивается по протоколу HTTP.
Сервис проверки статуса сертификата в режиме онлайн соответствует требованиям, описанным в OCSP RFC 2560. Квитанции с результатом проверки сертификата в режиме онлайн заверяются ЭЦП службы OCSP.

4.11 Окончание срока действия сертификата

Регистрационное свидетельство подписчика УЦ становится недействительным по истечении срока действия.
Подписчик вправе отозвать регистрационное свидетельство до окончания срока его действия в соответствии с пунктом 4.9 настоящего Регламента.

5 УПРАВЛЕНИЕ, ОПЕРАЦИОННЫЙ И ФИЗИЧЕСКИЙ КОНТРОЛЬ

5.1 Физические меры обеспечения безопасности

5.1.1 Размещение Удостоверяющего Центра

Информационная система удостоверяющего центра, обрабатывающая запросы участников УЦ, расположена в специализированных центрах обработки данных.

5.1.2 Физический доступ

Физический доступ в основной и резервный центры обработки данных организованы и контролируются одинаковыми мерами безопасности. Серверные помещения оборудованы системами:
1) контроля и управления доступом;
2) охранной сигнализации;
3) видеонаблюдения;
4) гарантированного электропитания;
5) электрического заземления;
6) обеспечения микроклимата;
7) пожарной сигнализации;
8) газового автоматического пожаротушения.

5.1.3 Хранение носителей архивной информации

Удостоверяющий центр ведет архив в соответствии с действующим внутренним документом Банка, регламентирующем резервное копирование и восстановление информации.

5.1.4 Уничтожение электронных носителей

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

5.1.5 Резервное копирование вне сети

Не определено.

5.2 Организационные меры обеспечения безопасности

5.2.1 Разграничение ролей (полномочий)

Роли участников и работников УЦ:
- Администратор УЦ;
- Пользователь УЦ;
- Аудитор УЦ.

5.3 Требования к персоналу

5.3.1 Требования к квалификации персонала

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

5.3.2 Процедура проверки работников

Проверка работников осуществляется в соответствии с внутренними инструкциями службы безопасности Банка.

5.3.3 Требования к повышению квалификации персонала

Специалисты и руководители Удостоверяющего центра проходят обучение или сертификацию не реже одного раза в три года.

5.3.4 Частота и последовательность смены деятельности работников

Не определено.

5.3.5 Ответственность за нарушения

Персонал УЦ и Центры Регистрации несут ответственность за свои действия в соответствии с внутренними нормативными документами Банка и действующим законодательством Республики Казахстан.

5.3.6 Требования к независимым подрядчикам

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

5.3.7 Документация, предоставляемая персоналу

Деятельность работников УЦ регламентирована должностными инструкциями и внутренними нормативными документами Банка.
Доступ работников УЦ к документам и документации, составляющей документальный фонд УЦ, организован в соответствии с должностными инструкциями и функциональными обязанностями.

5.4 Порядок ведения записей аудита

5.4.1 Типы событий, подлежащих аудиту

УЦ обеспечивает протоколирование следующих событий:
- запрос на выпуск сертификата;
- запрос на отзыв сертификат;
- формирование закрытого ключа ЭЦП облачной ЭЦП;
- использование закрытого ключа ЭЦП облачной ЭЦП;
- удаление (стирание) закрытого ключа ЭЦП облачной ЭЦП.

Срок хранения протоколов работы составляет один год с даты истечения срока действия регистрационного свидетельства.
При протоколировании действий записывается следующая информация:
- дата, время;
- DN имя владельца сертификата;
- событие.

5.4.2 Частота анализа журналов аудита

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

5.4.3 Срок хранения журналов аудита

Срок хранения архива журналов аудита определяется в соответствии с требованиями «Правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре».

5.4.4 Защита журналов аудита

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

5.4.5 Резервное копирование журналов аудита

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

5.4.6 Условия сбора данных для аудита

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

5.4.7 Уведомление субъекта события, вносимого в журнал аудита

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

5.4.8 Анализ уязвимостей событий

События, записываемые в журнал аудита, также служат для анализа уязвимостей УЦ. УЦ проводит анализ уязвимостей и предотвращает их возможные проявления. Все найденные уязвимости и принятые меры по их устранению включаются в ежегодный отчет об аудите.

5.5 Ведение архива

5.5.1 Типы регистрируемых событий

УЦ ведет архив:
- журналов аудита в соответствии с подразделом 5.4;
- сертификатов пользователей УЦ, срок действия которых истек;
- отозванных сертификатов пользователей УЦ;
- СОРС УЦ;
- протоколов работы программного обеспечения УЦ.

5.5.2 Срок хранения архива

УЦ хранит архив на протяжении всего срока работы.

5.5.3 Защита архива

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

5.5.4 Требования к простановке времени создания архивных записей

Не определено.

5.5.5 Условия архивирования

УЦ обеспечивает ведение архива в соответствии с законодательством Республики Казахстан.

5.5.6 Порядок получения и проверки информации, хранящейся в архиве

Доступ к архиву имеют только уполномоченные работники Центра Сертификации.

5.6 Смена ключей Центра Сертификации

Заблаговременно, до окончания срока действия закрытого ключа уполномоченного лица Центра Сертификации, администратор Центра производит формирование нового закрытого ключа и сертификата уполномоченного лица Центра Сертификации и публикует его в соответствующий раздел хранилища сертификатов.
По окончании действия закрытого ключа, носители ключевой информации с закрытым ключом и его копиями уничтожаются по акту.

5.7 Восстановление в случае компрометации или сбоев

5.7.1 Действия по предотвращению компрометации и сбоев

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

5.7.2 Случаи повреждения оборудования, программных и/или аппаратных сбоев

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

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

5.7.3 Компрометация ключа участника информационной системы

В случае если секретный ключ потерян или есть основания полагать, что информация о секретном ключе стала доступной третьим лицам, требуется немедленно направить в УЦ запрос на отзыв сертификата.

5.7.4 Восстановление работоспособности после аварии

Случаи повреждения вычислительных, программных ресурсов и/или данных информационной системы Удостоверяющего центра обрабатываются в соответствии с внутренним нормативным документом Банка, устанавливающим порядок действий работников Удостоверяющего центра в нештатных и кризисных ситуациях.

5.8 Разрешение конфликтных ситуаций

5.8.1 Непризнание ЭЦП электронного документа его целостности и подлинности

Споры между участниками инфраструктуры открытых ключей: между владельцами сертификатов и доверяющими сторонами, а также между владельцем сертификата или доверяющей стороной, с одной стороны, и Удостоверяющим центром или Центром регистрации, с другой стороны, – разрешаются в соответствии с положениями законодательства Республики Казахстан и договоров, действующих между сторонами (при наличии).
Если спор не решен в досудебном порядке, то он подлежит разрешению в судебном порядке.
Для разрешения споров, предметом которых являются разногласия по существу Регламента, применяется законодательство Республики Казахстан.

5.8.2 Процедура проверки ЭЦП документа

Процедура проверки ЭЦП электронного документа включает в себя проверку действительности использования сертификата на момент подписания, проверку подлинности ЭЦП и проверку соответствия использования ЭЦП сведениям в сертификате используя действующие "Правила проверки подлинности электронной цифровой подписи".

6 ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

6.1 Изготовление и установка ключевой пары

6.1.1 Изготовление ключей и используемые алгоритмы

Создание закрытых ключей ЭЦП проводится уполномоченным работником Банка, на основании заявления на выпуск сертификата.
Ключи ЭЦП формируются на электронных носителях ключевой информации в сертифицированном криптографическом модуле и не могут быть извлечены в незащищенном виде.
Ключи ЭЦП формируются в соответствии с алгоритмом ГОСТ 34.310–2004.
Закрытые ключи подписчиков УЦ облачной ЭЦП создаются строго внутри HSM модуля. Закрытый ключ облачной ЭЦП не извлекается из HSM в открытом виде.
Требования к HSM модулям облачного УЦ:
- не ниже третьего уровня безопасности в соответствии с требованиями, установленными СТ РК 1073–2007 "Средства криптографической защиты информации. Общие технические требования";
- спроектирован с физической защитой периметра (защита от вскрытия корпуса), использующей датчики для определения факта вскрытия корпуса и последующего удаления ключевой информации, необходимой для HSM;
- соответствует нормам эффективности защиты и методикам оценки защищенности информации и технических средств согласно требованиям действующего законодательства Республики Казахстан.
Ключи облачной ЭЦП формируются в соответствии с алгоритмом ГОСТ 34.310–2004.

6.1.2 Передача закрытого ключа подписи владельцу

Не предусмотрена.

6.1.3 Передача открытых ключей подписей доверяющим сторонам

УЦ публикует сертификаты и СОРС в соответствии с порядком, описанном в настоящем Регламенте. До начала использования сертификата участник информационной системы имеет возможность ознакомиться с сертификатами УЦ. Ознакомившись с сертификатами УЦ, пользователь подтверждает свое полное и безоговорочное согласие с условиями использования сервисов УЦ.

6.1.4 Размеры ключей

При использовании криптографического преобразования по алгоритму ГОСТ 34.310–2004:
- закрытый ключ – 256 бит;
- открытый ключ – 512 бит.

6.1.5 Параметры генерации и проверки качества закрытого ключа

Определяются сертифицированным в соответствии с СТ РК 1073–2007 СКЗИ автоматически.

6.1.6 Цели использования ключа

Заполняются в соответствии с политикой сертификата. Значения поля «Key Usage» сертификата УЦ:
- цифровая подпись;
- неотрекаемость.

6.1.7 Требования к носителям ключевой информации

УЦ сертифицирован для применения электронных носителей ключевой информации и имеет техническую возможность работы со следующими носителями ключевой информации:
- SafeNet 5100;
- SafeNet 5110;
- KAZTOKEN;
- KAZTOKEN смарт-карта.

6.1.8 Резервное копирование закрытого ключа

Резервное копирование закрытого ключа пользователя не предусмотрено.
Резервное копирование закрытого ключа Центра Сертификации происходит в соответствии с эксплуатационной документацией HSM модулей и СКЗИ по схеме n из m. Резервная копия закрытого ключа Центра Сертификации хранится отдельно от криптографического модуля в зашифрованном архиве.

6.1.9 Архивирование закрытого ключа

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

6.1.10 Запись закрытого ключа в носитель ключевой информации

Производится штатными средствами модуля криптографической защиты информации в соответствии с эксплуатационной документацией.

6.1.11 Хранение закрытого ключа в электронном носителе ключевой информации

Закрытые ключи хранятся только в зашифрованном виде и не покидают криптографический модуль иначе как в зашифрованном архиве.

6.2 Другие особенности использования ключей

6.2.1 Архивирование открытых ключей подписей

Все сертификаты архивируются в соответствии с порядком резервного копирования, установленным в УЦ.

6.2.2 Распространение открытого ключа Центра Сертификации

Предоставление открытого ключа Центра Сертификации реализовано посредством публикации его сертификата в хранилище и на сайте Центра Сертификации.
Безопасность сертификата Центра Сертификации реализована путем предоставления информации о серийном номере сертификата и его хэш значения, с предоставлением доверяющим сторонам возможности его проверки.
В случае смены ключей подписи Центра Сертификации и выпуска нового сертификата Центра Сертификации его распространение может производиться с использованием механизма кросс-сертификации.

6.2.3 Сроки действия сертификатов и ключей

Начало периода действия сертификата Центра Сертификации исчисляется с даты и времени его генерации. Срок действия сертификата УЦ составляет 20 лет.
Срок действия пользовательского сертификата составляет один календарный год. Начало периода действия закрытого ключа владельца сертификата исчисляется с даты и времени начала действия соответствующего сертификата.

6.2.4 Ограничения на использования ключей

Закрытый ключ Центра Сертификации используется для формирования ЭЦП сертификатов открытых ключей пользователей и СОРС.
Закрытые ключи пользователей УЦ используются для формирования ЭЦП электронных документов и подписании в информационных системах Банка.

6.3 Данные активации закрытых ключей

6.3.1 Генерация и установка данных активации закрытого ключа

При установке пароля на ключевой контейнер участник УЦ обязан создать пароль, при этом пароль должен содержать:
- латинские буквы, в верхнем и нижнем регистре;
- минимум одну цифру;
- минимум один спецсимвол;
- минимум 8 символов.

6.3.2 Защита данных активации закрытого ключа

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

6.3.3 Особенности данных активации закрытого ключа

Не определено.

6.4 Средства управления компьютерной безопасностью

6.4.1 Специфические технические требования к компьютерной безопасности

Требования к серверам ИОК:
- обеспечение мер отказоустойчивости и безопасности;
- ежегодное сканирование безопасности;
- мониторинг ресурсов.

Компьютеры уполномоченных лиц УЦ должны удовлетворять следующим требованиям:
- использование лицензионного программного обеспечения;
- операционные системы поддерживаются на высоком уровне защиты, при регулярном применении всех рекомендованных и соответствующих пакетов защиты, в том числе антивирусов и межсетевых экранов;
- недопустимость совместного использования компьютера несколькими пользователями;
- на компьютере отсутствуют СКЗИ, отличные от определенных в данном Регламенте.

6.4.2 Оценка компьютерной безопасности

Не определено.

6.5 Технические средства управления жизненным циклом

6.5.1 Контроль работы системы

Не определено.

6.5.2 Средства управления безопасностью

Не определено.

6.5.3 Управление безопасностью жизненного цикла

Не определено.

6.6 Средства управления сетевой безопасностью

Безопасность аппаратных средств Центра Сертификации обеспечивается антивирусами и межсетевыми экранами.

6.7 Списание оборудования

Не определено.

7 ШАБЛОНЫ СЕРТИФИКАТОВ И CORC

7.1 Описание сертификата

7.1.1 Версия сертификата

Центр Сертификации выдает сертификаты, соответствующие рекомендациям X.509 ITU-T версии 3 и RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile».

7.1.2 Объектные идентификаторы алгоритмов

Центр Сертификации использует объектные идентификаторы Республики Казахстан (OID РК) https://root.gov.kz/oid/

7.1.3 Структура сертификата УЦ Банка (ГОСТ)

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

7.1.4 Структура сертификата уполномоченного лица Банка (ГОСТ)

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

7.1.5 Структура сертификата физического лица (ГОСТ)

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

7.2 Описание COPC

7.2.1 Структура COPC (ГОСТ)

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

7.2.2 Профиль OCSP

Протокол OCSP необходим доверяющим сторонам для определения статуса указанного сертификата в текущий момент времени. OCSP может использоваться для обеспечения требований,касающихся получения более своевременной информации об отмене, чем это возможно с использованием COPC.

7.2.3 Номер версии

УЦ формирует квитанции OCSP в электронной форме версии 1 в соответствии с RFC 6960 «Online Certificate Status Protocol – OCSP».

7.2.4 Расширения OCSP

Не определено.

8. ПРОЧИЕ ПОЛОЖЕНИЯ

8.1. Управление документом

Регламент актуализируется Дирекцией криптографической защиты информации Банка (Удостоверяющим центром), расположенным по адресу: A05G1D2, г. Алматы, ул. Панфилова, д. 98, блок Б.
Контактное лицо по вопросам актуализации документа – Руководитель Дирекции криптографической защиты информации Банка (Удостоверяющего центра), A05G1D2, г. Алматы, ул. Панфилова, д. 98, блок Б, +7 (727) 2-598-583 (вн. 12921), alexey.korobetskikh@bcc.kz.
Изменения и дополнения в Регламент готовятся Удостоверяющим центром либо в форме новой редакции документа, либо в форме перечня изменений и дополнений к текущей его редакции.
Перед утверждением изменения и дополнения в Регламент проходят согласование с заинтересованными подразделениями и должностными лицами Банка согласно внутренним процедурам.
Изменения и дополнения в Регламент утверждаются протокольным решением Правления Банка.
Все изменения и дополнения в Регламент публикуются на официальном информационном ресурсе Банка в сети Интернет по адресу https://www.bcc.kz/product/pki/?tab=DPP.
Публикация новой утвержденной редакции Регламента в разделе «Действующие редакции» является официальным уведомлением о вступлении ее в силу для всех владельцев регистрационных свидетельств, выпущенных Удостоверяющим центром, и всех доверяющих сторон.
С даты официального уведомления о вступлении в силу новой редакции Регламента, если иное не предусмотрено переходными положениями утверждающего решения, изменения и дополнения становятся обязательными для применения всеми владельцами регистрационных свидетельств, выпущенных Удостоверяющим центром, и всеми доверяющими сторонами.
Незначительные изменения в Регламент (изменение адресов и ссылок, контактной информации, исправление опечаток и пр.) вносятся без предварительного уведомления участников инфраструктуры открытых ключей. Решения об уровне значимости изменений и дополнений (существенные или несущественные) принимаются Удостоверяющим центром самостоятельно.
Существенные изменения и дополнения в Регламент Удостоверяющий центр предварительно публикует, в форме проекта, на официальном информационном ресурсе Банка в сети Интернет, как правило за 14 календарных дней до вступления в силу, если иное не предусмотрено опубликованными изменениями в законодательстве Республики Казахстан.

8.2 Разрешение споров

Для разрешения споров, предметом которых являются разногласия по существу Регламента, применяется законодательство Республики Казахстан.
Если спор не решен в досудебном порядке, то он подлежит разрешению в судебном порядке.
В случае если часть положений Регламента будет признана неприменимой судом или уполномоченным государственным органом, остальная их часть сохраняет силу.
В случае наступления обстоятельств непреодолимой силы (форс-мажор) участники инфраструктуры открытых ключей: Удостоверяющий центр, Центры регистрации, владельцы регистрационных свидетельств и доверяющие стороны руководствуются соответствующими положениями действующих между ними договоров (при наличии).

8.3. Ответственность

Ответственность участников инфраструктуры открытых ключей, обслуживаемой Удостоверяющим центром, установлена законодательством Республики Казахстан[1].
Ответственность персонала Удостоверяющего центра и Центров регистрации установлена трудовым

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

договором и должностными инструкциями.

8.4 Гарантии и заверения

Удостоверяющий центр 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 персонала Удостоверяющего центра;
2) соответствие оказываемых услуг (выпуск, отзыв регистрационных свидетельств, выпуск CORC, онлайн-сервисы OCSP и TSP, создание и защищенное хранение закрытых ключей ЭЦП, формирование ЭЦП по запросам владельца регистрационных свидетельств) требованиям: действующего законодательства Республики Казахстан по вопросам электронного документа и электронной цифровой подписи, Политики регистрационных свидетельств и Регламента;
3) публикацию требований Политики регистрационных свидетельств и Регламента на официальном информационном ресурсе Банка в сети Интернет.
Центры регистрации обеспечивают:
1) соответствие данных в направляемых в Удостоверяющий центр запросах на выпуск регистрационного свидетельства, сведениям из тех документов, которые предоставил заявитель в ходе процедур идентификации и аутентификации, и отсутствие в данных запросах умышленных или случайных искажений, внесенных по умыслу или допущенных в результате ошибочных действий персонала Центра регистрации;
2) соответствие выполняемых персоналом Центра регистрации процедур (регистрация и обработка заявлений на выпуск и отзыв регистрационных свидетельств, процедуры идентификации и аутентификации заявителей, выдача регистрационных свидетельств их владельцам) требованиям: действующего законодательства Республики Казахстан по вопросам электронного документа и электронной цифровой подписи, Политики регистрационных свидетельств и Регламента.

8.5 Отказ от гарантий и ограничение ответственности

Участники инфраструктуры открытых ключей не несут ответственности за непрямой, особый, случайный или вытекающий ущерб и упущенную выгоду.
Удостоверяющий центр не несет перед владельцами регистрационных свидетельств и доверяющими сторонами дополнительной ответственности, вытекающей из договоров оказания банковских услуг, включая ответственность за товарную пригодность и соответствие, кроме той ответственности, которая установлена законодательством Республики Казахстан по вопросам электронного документа и электронной цифровой подписи

8.6 Вступление в силу и прекращение действия

Регламент и все изменения и дополнения к нему вступают в силу не ранее дня опубликования на официальном ресурсе Банка в сети Интернет.
Регламент, с учетом публикуемых изменений и дополнений к нему, сохраняет силу до момента опубликования своей новой редакции на официальном ресурсе Банка в сети Интернет.
В случае отмены Регламента участники информационных систем, которые используют регистрационные свидетельства, выпущенные Удостоверяющим центром, остаются связанными требованиями Политики регистрационных свидетельств до момента истечения периода действия регистрационных свидетельств.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

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

Подразделения Банка, взаимодействующие с УЦ, несут ответственность:

1) за соблюдение требований, описанных в данном Регламенте;
2) за полноту и своевременность исполняемых функций в рамках своих полномочий.

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

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

Дирекция криптографической защиты информации

Приложение 1
к Регламенту
Удостоверяющего Центра

ЗАЯВЛЕНИЕ
на выдачу регистрационного свидетельства от физического лица

Индивидуальный идентификационный номер: _____

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

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

Настоящим подтверждаю, что:

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

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

Приложение 2
к Регламенту
Удостоверяющего Центра

ЗАЯВЛЕНИЕ
на отзыв регистрационного свидетельства от физического лица

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

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

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