

Приложение
к Постановлению Совета Директоров
№1106/4 от 06.11.2024 г.

**ПОЛИТИКА ПРИМЕНЕНИЯ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА АО «БАНК ЦЕНТРКРЕДИТ»**

Версия 2.1.1

Алматы 2024

Оглавление

Раздел 1. ВВЕДЕНИЕ	4
Глава 1.1. Общие положения	4
Глава 1.2 Наименование и атрибуты документа	5
Глава 1.3 Участники инфраструктуры открытых ключей.....	5
1.3.1 Центр сертификации	5
1.3.2 Центр регистрации.....	5
1.3.3 Владелец регистрационного свидетельства	5
1.3.4 Доверяющая сторона	5
Глава 1.4 Назначение регистрационных свидетельств	6
Глава 1.5 Управление документом	6
Глава 1.6 Термины, определения и сокращения	7
Раздел 2. ОТВЕТСТВЕННОСТЬ ЗА ХРАНИЛИЩЕ И ПУБЛИКАЦИЮ ДАННЫХ В НЕМ	9
Глава 2.1 Хранилище	9
Глава 2.2 Публикация в хранилище информации о регистрационных свидетельствах	9
Глава 2.3 Периодичность актуализации данных в хранилище	9
Глава 2.4 Контроль доступа к хранилищу	9
Раздел 3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ	9
Глава 3.1 Требования к именам	9
Глава 3.2 Первоначальная проверка идентичности	9
3.2.1 Идентификация и аутентификация при выпуске регистрационного свидетельства для обслуживаемых физических лиц	9
3.2.2 Идентификация и аутентификация при выпуске технологического регистрационного свидетельства (для служебных пользователей УЦ).....	10
Глава 3.3. Идентификация и аутентификация при запросах на смену ключей электронной цифровой подписи	10
Глава 3.4. Идентификация и аутентификация при отзыве регистрационного свидетельства	10
3.4.1. Идентификация и аутентификация при отзыве регистрационного свидетельства для обслуживаемых лиц	10
3.4.2. Идентификация и аутентификация при отзыве технологического регистрационного свидетельства (для служебных пользователей УЦ).....	10
Раздел 4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА	10
Глава 4.1 Заявки на выдачу регистрационного свидетельства	10
Глава 4.2 Обработка заявок на выдачу регистрационного свидетельства	10
Глава 4.3 Выпуск регистрационных свидетельств.....	10
Глава 4.4 Принятие регистрационных свидетельств	11
Глава 4.5 Использование регистрационных свидетельств и ключевых пар	11
Глава 4.6 Обновление сроков действия регистрационного свидетельства	11
Глава 4.7 Смена ключей электронной цифровой подписи в регистрационном свидетельстве	11
Глава 4.8 Изменение сведений, указанных в регистрационном свидетельстве	11
Глава 4.9 Отзыв и приостановление действия регистрационного свидетельства	11

Раздел 5 ФИЗИЧЕСКИЙ, ОПЕРАЦИОННЫЙ И УПРАВЛЯЮЩИЙ КОНТРОЛИ	11
Глава 5.1 Физический контроль.....	11
Глава 5.2 Операционный контроль	11
Глава 5.3 Контроль персонала	11
Глава 5.4 Процедуры контрольного протоколирования и управления инцидентами информационной безопасности.....	11
Глава 5.5 Ведение архива	12
Глава 5.6 Смена ключей электронной цифровой подписи Центра сертификации	12
Глава 5.7. Восстановление функционирования в случае компрометации или сбоя	12
Глава 5.8 Прекращение работы Удостоверяющего центра	12
Раздел 6 ТЕХНИЧЕСКИЙ КОНТРОЛЬ БЕЗОПАСНОСТИ	12
Глава 6.1 Изготовление и установка ключевых пар электронной цифровой подписи	12
Глава 6.2 Защита закрытого ключа электронной цифровой подписи и инженерные контроли аппаратных криптографических модулей	12
Глава 6.3 Другие особенности управления ключами электронной цифровой подписи	12
Глава 6.4 Данные активации	12
Глава 6.5 Контроль безопасности вычислительных ресурсов	12
Раздел 7 ПРОФИЛИ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ, СПИСКОВ ОТОЗВАННЫХ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ И СЕРВИСА ПРОТОКОЛА ПРОВЕРКИ СТАТУСА РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ В РЕЖИМЕ ОНЛАЙН.....	13
Глава 7.1 Профили регистрационных свидетельств	13
Глава 7.2 Профиль списка отозванных регистрационных свидетельств	13
Глава 7.3 Профиль сервиса протокола проверки статуса регистрационных свидетельств в режиме онлайн	13

Раздел 1. ВВЕДЕНИЕ

Глава 1.1. Общие положения

1. Настоящая Политика применения регистрационных свидетельств удостоверяющего центра АО «Банк ЦентрКредит» (далее – Политика регистрационных свидетельств) разработана 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).

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

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

- 1) Закон Республики Казахстан «Об информатизации»;
- 2) Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи»;
- 3) Закон Республики Казахстан «О персональных данных и их защите»;
- 4) правовой акт по вопросам создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющих центрах¹ (далее – Правила облачной ЭЦП);
- 5) правовой акт по вопросам проверки подлинности электронной цифровой подписи²;
- 6) правовой акт по вопросам выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющими центрами³ (далее – Правила выпуска и отзыва регистрационных свидетельств);

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

4. Политика регистрационных свидетельств определяет виды регистрационных свидетельств, выпускаемых Удостоверяющим центром, основные принципы и общие требования их применимости в заинтересованных информационных системах, объединенных типовыми требованиями информационной безопасности, что гарантирует определенный уровень доверия в информационных системах, использующих эти регистрационные свидетельства.

5. Политика регистрационных свидетельств не определяет детальный порядок и процедуры функционирования Удостоверяющего центра, обеспечения безопасности инфраструктуры открытых ключей, которые согласно требованиям правовых актов Республики Казахстан и международных отраслевых рекомендаций RFC 3647, вынесены в отдельный внутренний нормативный документ АО «Банк ЦентрКредит» (далее – Регламент деятельности Удостоверяющего центра).

6. С момента подачи (подписания) участником информационной системы, использующей сервисы Удостоверяющего центра, электронной заявки (заявления) на выдачу регистрационного свидетельства, для участника становятся обязательными к выполнению применимые к нему требования Политики регистрационных свидетельств и Регламента деятельности Удостоверяющего центра, ссылка на которые содержится в электронной заявке (заявлении).

На дату утверждения Политики регистрационных свидетельств действуют:

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

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

³ Правила выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром, за исключением корневого удостоверяющего центра Республики Казахстан, удостоверяющего центра государственных органов, национального удостоверяющего центра Республики Казахстан и доверенной третьей стороны Республики Казахстан, в редакции с изменениями, внесенными приказом и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 30 марта 2023 года № 115/НК.

Глава 1.2 Наименование и атрибуты документа

7. Полное наименование документа – Политика применения регистрационных свидетельств удостоверяющего центра АО «Банк ЦентрКредит».
8. Объектный идентификатор – 1.2.398.3.24.1.1.1.
9. Версия документа – 2.1.1.
10. Адрес сервера для публикации документа – <https://www.bcc.kz/product/pki/?tab=DPP>.

Глава 1.3 Участники инфраструктуры открытых ключей

1.3.1 Центр сертификации

11. Центр сертификации – в контексте Политики регистрационных свидетельств данным термином обозначается программно-аппаратный комплекс для выпуска, обслуживания и отзыва регистрационных свидетельств, аккредитованный в соответствии с законодательством и действующий в соответствии с утвержденным Регламентом деятельности Удостоверяющего центра.

12. Центр сертификации осуществляет следующие функции инфраструктуры открытых ключей:

- 1) обработка запросов на выпуск и отзыв регистрационных свидетельств;
 - 2) публикация списков отозванных регистрационных свидетельств;
 - 3) обработка запросов к службе протокола проверки статуса регистрационного свидетельства в режиме онлайн;
 - 4) обработка запросов к службе протокола метки времени.
13. Маркировка Центра сертификации в регистрационных свидетельствах:
C = KZ,
O = Bank CenterCredit JSC,
CN = Certification Authority

1.3.2 Центр регистрации

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

1.3.3 Владелец регистрационного свидетельства

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

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

1.3.4 Доверяющая сторона

17. Доверяющая сторона – в контексте Политики регистрационных свидетельств данным термином обозначается владелец регистрационного свидетельства или любое другое физическое лицо, использующее в информационных системах АО «Банк ЦентрКредит» регистрационные свидетельства, выпущенные Удостоверяющим центром, и/или электронные документы с электронными цифровыми подписями, подлинность которых проверяется с помощью этих регистрационных свидетельств.

Глава 1.4 Назначение регистрационных свидетельств

18. Целью выпуска регистрационных свидетельств Удостоверяющим центром является обеспечение потребностей информационных систем, принадлежащих АО «Банк ЦентрКредит».

19. При этом Удостоверяющий центр запрещает использование выпущенных им регистрационных свидетельств в информационных системах, связанных с управлением источниками повышенной опасности (ядерным, аэронавигационным оборудованием, системами контроля вооружений и др.), а также в иных информационных системах в любых случаях, когда ошибка при принятии решения о доверии, основанном на регистрационном свидетельстве, может повлечь за собой ранение или смерть персонала, или ущерб окружающей среде.

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

21. Область допустимого применения регистрационного свидетельства, выпущенного Удостоверяющим центром, может дополнительно ограничиваться с помощью его расширения «certificatePolicies», которое предназначено для отражения объектных идентификаторов политики применения регистрационного свидетельства.

22. Наличие объектных идентификаторов политики в расширении «certificatePolicies» дает информационным системам, использующим регистрационные свидетельства, возможность дополнительной защиты в форме контроля системой наборов необходимых и запрещенных объектных идентификаторов политики с ограничением применения неподходящих регистрационных свидетельств.

23. Не допускается использование регистрационных свидетельств, выпущенных Удостоверяющим центром, способами, противоречащими законодательству Республики Казахстан, Политике регистрационных свидетельств, Регламенту деятельности Удостоверяющего центра.

24. Регистрационные свидетельства, выданные Удостоверяющим центром их владельцам, используются для работы с программным обеспечением доверяющих сторон и не используются как технологические регистрационные свидетельства информационной системы Удостоверяющего центра. В свою очередь технологические регистрационные свидетельства информационной системы Удостоверяющего центра не используются ни для каких иных целей кроме их прямого функционального назначения.

Глава 1.5 Управление документом

25. Политика регистрационных свидетельств актуализируется Дирекцией криптографической защиты информации (Удостоверяющим центром), расположенным по адресу: А05G1D2, г. Алматы, ул. Панфилова, д. 98, блок Б.

26. Контактное лицо по вопросам актуализации документа – Руководитель Дирекции криптографической защиты информации (Удостоверяющего центра), А05G1D2, г. Алматы, ул. Панфилова, д. 98, блок Б, +7 (727) 2-598-583 (вн. 12921), alexey.korobetskikh@bcc.kz.

27. Изменения и дополнения в Политику регистрационных свидетельств готовятся Удостоверяющим центром либо в форме новой редакции документа, либо в форме перечня изменений и дополнений к текущей его редакции.

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

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

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

31. С даты официального уведомления о вступлении в силу новой редакции Политики регистрационных свидетельств, 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.

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

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

Глава 1.6 Термины, определения и сокращения

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

35. Значение и применение терминов «Центр сертификации», «Центр регистрации», «доверяющая сторона», а также особенности применения в документе термина «владелец регистрационного свидетельства» приведены в Главе 1.3. Регламента деятельности Удостоверяющего центра.

36. Другие специальные термины, применяемые в Политике регистрационных свидетельств, используются в следующем значении:

Термин	Определение
Аппаратный криптографический модуль (Hardware Security Module)	Аппаратный криптографический модуль, предназначенный для шифрования информации и управления открытыми и закрытыми ключами электронной цифровой подписи.
Аутентификация	Процесс или сервис безопасности, реализующий этот процесс, который предназначен для проверки того, что лицо (предмет) является тем, кем себя именует (чем он поименован)
Банк	АО «Банк ЦентрКредит»
Биометрическая аутентификация	Комплекс мер, идентифицирующих личность на основании физиологических и неизменных биологических признаков
Данные активации	Любые данные, за исключением целых криптографических ключей, которые необходимы для выполнения криптографических преобразований и требуют защиты: персональные идентификационные номера (PIN), парольные фразы, компоненты разделенного криптографического ключа, биометрические параметры и др.
Заявитель	Физическое лицо, подавшее документы на выдачу или отзыв регистрационного свидетельства
Идентификация	Процесс (или результат процесса), который устанавливает идентичность физического или юридического лица (показывающий, что данное лицо является однозначно определенным реально существующим лицом), и состоит из двух этапов: <ul style="list-style-type: none">установление соответствия, предъявленного лицом имени реально существующей идентичности лица иустановление того, что лицо, обращающееся за доступом к чему-либо от определенного имени, на самом деле является тем лицом, которым себя именует (аутентификация)
Информационная система	Организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач

Термин	Определение
Инфраструктура открытых ключей	Набор сил и средств (технических, материальных, людских и пр.), распределённых служб и компонентов, в совокупности используемых для решения криптографических задач (аутентификации, шифрования, контроля целостности и доказательности) на основе криптосистем с открытым ключом, способный самостоятельно обеспечить управление открытыми ключами, посредством которых решаются указанные задачи
Компрометация ключей электронной цифровой подписи	Утрата владельцем регистрационного свидетельства уверенности в том, что конкретные ключи электронной цифровой подписи обеспечивают безопасность защищаемой с их помощью информации
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)
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 удаленно посредством не менее двух факторов аутентификации, одним из которых является биометрическая
Объект	Алгоритм, информационная система, а также другие элементы, используемые физическими и юридическими лицами для электронного документооборота
Объектный идентификатор	Уникальный набор цифр, который связан с объектом и однозначно идентифицирует его в мировом адресном пространстве объектов
Отозванное регистрационное свидетельство	Регистрационное свидетельство, аннулированное в порядке, который установлен Правилами выпуска и отзыва регистрационных свидетельств
Политика применения регистрационных свидетельств	Внутренний документ, утвержденный удостоверяющим центром, определяющий регламент и механизмы работы удостоверяющего центра в части управления регистрационными свидетельствами
Приложение ВСС	Мобильные приложения/цифровые платформы Банка, предоставляющие услуги дистанционного банковского обслуживания для физических лиц
Протокол метки времени	Криптографический протокол, позволяющий создавать доказательство факта существования электронного документа на определённый момент времени
Регламент деятельности удостоверяющего центра	Документ, который определяет порядок организации основной деятельности удостоверяющего центра, осуществляемой в соответствии с политикой применения регистрационных свидетельств, включая реализацию основных процессов удостоверяющего центра
Список отозванных регистрационных свидетельств	Часть регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва (аннулирования)
Участники инфраструктуры открытых ключей	Совокупность физических и юридических лиц, которые выполняют любую из ролей в одной и той же инфраструктуре открытых ключей: роль владельца регистрационного свидетельства или доверяющей стороны, – а также удостоверяющего центра и центра(-ов) регистрации

37. В тексте Политики регистрационных свидетельств используются следующие сокращения:

Аббревиатура	Определение
DN	Отличительное имя (Distinguished Name)
HSM	Аппаратный криптографический модуль (Hardware Security Module)
LDAP	Протокол облегченного доступа к каталогам (Lightweight Directory Access Protocol)
OCSP	Протокол проверки статуса регистрационного свидетельства в режиме онлайн (Online Certificate Status Protocol)
OID	Объектный идентификатор (Object Identifier)
TSP	Протокол метки времени (Time Stamp Protocol)
ИОК	Инфраструктура открытых ключей
ИС	Информационная система
СОПС	Список отозванных регистрационных свидетельств
УЦ	Удоcтoверяющий центр АО «Банк ЦентрКредит»
ЭЦП	Электронная цифровая подпись

Раздел 2. ОТВЕТСТВЕННОСТЬ ЗА ХРАНИЛИЩЕ И ПУБЛИКАЦИЮ ДАННЫХ В НЕМ

Глава 2.1 Хранилище

38. УЦ предоставляет для скачивания и ознакомления следующие документы:

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

39. Через приложение ВСС пользователям приложения, а также работникам центра регистрации обеспечивается доступность подачи запросов к следующим сервисам УЦ:

- 1) ОССП <https://bcc-app.bank.corp.centercredit.kz:62301/>
- 2) TSP <https://bcc-app.bank.corp.centercredit.kz:62302/>
- 3) Центр сертификации <https://bcc-app.bank.corp.centercredit.kz:62305/>
- 4) Центр регистрации <https://bcc-app.bank.corp.centercredit.kz:62310/>

Глава 2.2 Публикация в хранилище информации о регистрационных свидетельствах

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

Глава 2.3 Периодичность актуализации данных в хранилище

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

42. Публикация СОРС производится по мере появления отозванных регистрационных свидетельств. При этом период обновления СОРС не превышает 7 (семь) календарных дней.

43. Сведения о статусе регистрационного свидетельства публикуются в соответствии с Политикой регистрационных свидетельств.

Глава 2.4 Контроль доступа к хранилищу

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

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

Раздел 3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Глава 3.1 Требования к именам

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

47. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 3.2 Первоначальная проверка идентичности

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

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

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

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

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

50. Процедуры идентификации и аутентификации при обработке электронной заявки (заявления) и смене ключей ЭЦП полностью аналогичны процедурам идентификации и аутентификации при обработке электронной заявки (заявления) и выпуске регистрационного свидетельства, изложенным в Главе 3.2.

Глава 3.4. Идентификация и аутентификация при отзыве регистрационного свидетельства

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

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

- 1) пройти процедуру биометрической аутентификации;
- 2) ввести пароль от закрытого ключа ЭЦП, соответствующего регистрационному свидетельству, и указать причину отзыва.

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

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

Раздел 4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА

Глава 4.1 Заявки на выдачу регистрационного свидетельства

53. Заявку на выдачу регистрационного свидетельства имеют право подавать физические лица, имеющие индивидуальный идентификационный номер в национальном реестре Республики Казахстан.

54. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 4.2 Обработка заявок на выдачу регистрационного свидетельства

55. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 4.3 Выпуск регистрационных свидетельств

56. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 4.4 Принятие регистрационных свидетельств

57. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 4.5 Использование регистрационных свидетельств и ключевых пар

58. Регистрационные свидетельства, выданные УЦ, применимы для проверки ЭЦП.

59. Закрытые ключи, соответствующие регистрационным свидетельствам владельцев, выпущенным УЦ, предназначены для формирования ЭЦП.

60. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 4.6 Обновление сроков действия регистрационного свидетельства

61. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 4.7 Смена ключей электронной цифровой подписи в регистрационном свидетельстве

62. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 4.8 Изменение сведений, указанных в регистрационном свидетельстве

63. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 4.9 Отзыв и приостановление действия регистрационного свидетельства

64. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Раздел 5 ФИЗИЧЕСКИЙ, ОПЕРАЦИОННЫЙ И УПРАВЛЯЮЩИЙ КОНТРОЛИ

Глава 5.1 Физический контроль

65. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 5.2 Операционный контроль

66. УЦ обеспечивает меры информационной безопасности в соответствии с:

- 1) законодательством Республики Казахстан;
- 2) внутренними нормативными документами Банка;
- 3) должностными инструкциями работников Банка.

67. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 5.3 Контроль персонала

68. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 5.4 Процедуры контрольного протоколирования и управления инцидентами информационной безопасности

69. УЦ обеспечивает протоколирование следующих событий:

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

70. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 5.5 Ведение архива

71. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 5.6 Смена ключей электронной цифровой подписи Центра сертификации

72. УЦ осуществляет смену своих ключевых пар и регистрационных свидетельств в связи с истечением срока действия корневого регистрационного свидетельства или в случае компрометации соответствующих ему ключей ЭЦП.

73. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 5.7. Восстановление функционирования в случае компрометации или сбоя

74. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 5.8 Прекращение работы Удостоверяющего центра

75. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Раздел 6 ТЕХНИЧЕСКИЙ КОНТРОЛЬ БЕЗОПАСНОСТИ

Глава 6.1 Изготовление и установка ключевых пар электронной цифровой подписи

76. УЦ выпускает ключи и регистрационные свидетельства в соответствии с алгоритмом ГОСТ 34.310–2004.

77. Более подробная информация изложена в Регламенте деятельности удостоверяющего центра.

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

78. Закрытые ключи Центра сертификации создаются в HSM, сертифицированных на соответствие Стандарту по уровню не ниже второго.

79. Закрытые ключи пользователей ИС Банка – владельцев регистрационных свидетельств создаются в HSM, сертифицированных на соответствие Стандарту по уровню не ниже третьего.

80. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 6.3 Другие особенности управления ключами электронной цифровой подписи

81. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 6.4 Данные активации

82. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 6.5 Контроль безопасности вычислительных ресурсов

83. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

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

Глава 7.1 Профили регистрационных свидетельств

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

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

86. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 7.2 Профиль списка отозванных регистрационных свидетельств

87. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.

Глава 7.3 Профиль сервиса протокола проверки статуса регистрационных свидетельств в режиме онлайн

88. Более подробная информация изложена в Регламенте деятельности Удостоверяющего центра.