Евразийский Банк

Утверждены Правлением
АО «Евразийский банк»
протокол №141-09
от «12» Октября 2020 г.

для широкого пользования

ПРАВИЛА
ДЕЯТЕЛЬНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

ПР

Правила деятельности Удостоверяющего центра (далее – Правила) разработаны в соответствии с Постановлением Правления Национального Банка Республики Казахстан (далее – НБРК) от 27 марта 2018 года № 48 «Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах, постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», Законом Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи» (далее - Закон), рекомендациями RFC 3647 (Certificate Policy and Certification Practices Framework), RFC 2251 (Lightweight Directory Access Protocol), RFC 2560 (Online Certificate Status Protocol – OCSP), RFC 3161 (Time-Stamp Protocol – TSP), RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile), приказом и.о. Министра культуры и спорта Республики Казахстан от 29 сентября 2017 года № 263 «Об утверждении Перечня типовых документов, образующихся в деятельности государственных и негосударственных организаций, с указанием сроков хранения» (далее – Перечень), Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 1 июня 2020 года № 224/НҚ об утверждении Правил выдачи и отзыва свидетельства об аккредитации удостоверяющих центров, приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НҚ «Об утверждении Правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре», приказом Министра по инвестициям и развитию Республики Казахстан от 23 декабря 2015 года № 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», а так же внутренними нормативными документами (далее – ВНД) АО «Евразийский банк» (далее – Банк), в том числе Политикой внутреннего нормативного регулирования.

Раздел 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Правила описывают порядок предоставления услуг принадлежащего Банку Удостоверяющего центра (далее –УЦ) и правила его использования участниками УЦ. Описание процесса представлено в приложении №5 (SIPOC). Бизнес-владельцем процесса является Блок ИТ.
2. Правила являются соглашением, налагающим обязательства на все вовлеченные стороны, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ. Любой участник УЦ принимает Правила с момента начала использования УЦ.
3. Правила определяют требования, механизмы и условия предоставления и использования услуг УЦ, включая права, обязанности и ответственность участников УЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, включая, но, не ограничиваясь такими операциями, как выпуск, использование и отзыв регистрационных свидетельств (далее – РС) открытых ключей.
4. В Правилах используются основные понятия, предусмотренные законодательством РК, электронным справочником, а также следующие термины:

1) 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;
2) запрос – обращение к информационной системе УЦ с целью получения соответствующей услуги и/или информации;
3) заявитель – физическое, либо юридическое лицо, направившее заявление на выпуск РС;
4) компрометация ключа - утрата доверия к тому, что используемые владельцем ключи обеспечивают безопасность информации;

5) 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;

6) подразделение ИТ безопасности (далее – ПИТБ) – подразделение, отвечающее за обеспечение информационной безопасности УЦ;

7) Политика применения регистрационных свидетельств (далее – Политика) - является неотъемлемой частью Правил и определяет виды Регистрационных свидетельств, выпускаемых УЦ, процедуры их проверки и их применимость. Политика размещена на интернет-ресурсе https://eubank.kz/policy-of-application-of-registration-certificates/;

8) регистрация участника УЦ – внесение регистрационной информации о владельце РС в хранилище УЦ;

9) регистрационное свидетельство – электронный документ, выдаваемый УЦ для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом;

10) средства криптографической защиты информации (далее - СКЗИ) – программное обеспечение или аппаратно-программный комплекс, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами шифрования;

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

12) статус РС – составное понятие, отражающее результат проверки действительности РС. Например, просрочен – не просрочен, отозван – не отозван;

13) хранилище РС –справочник всех РС и СОРС;

14) хеш-значение – значение, образуемое после применения преобразования по детерминированному алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины;

15) электронный документ – документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи;

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

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

18) администратор программного обеспечение (далее – ПО) УЦ - работник, ответственный за поддержание работоспособности технических и программных компонентов УЦ;

19) уполномоченное лицо Центра сертификации – работник ПИТБ, ответственный за выдачу РС ключей и управления ими;

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

21) 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);

22) аппаратный криптографический модуль (Hardware Security Module) (далее - HSM) - аппаратный криптографический модуль, предназначенный для шифрования информации и управления открытыми и закрытыми ключами РС;

23) удостоверяющий центр – юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства;

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

Раздел 2. ОСОБЕННЫЕ ПОЛОЖЕНИЯ
Глава 1. Участники УЦ

5. Участниками УЦ являются:

1) Центр Сертификации – автоматизированный комплекс настраиваемых служб для выдачи РС ключей и управления ими, действующий в соответствии с утвержденными политиками безопасности;

2) Центр Регистрации – компонент УЦ, предназначенная для выполнения операций по идентификации, аутентификации и проверки полномочий заявителя;

3) Хранилище РС и списков отозванных РС – справочник, используемый Центром Сертификации для получения доступа к РС, службе проверки РС, хранения архивной информации и других функций;

4) Владелец РС – физическое или юридическое лицо, на имя которого Центром Сертификации выдан РС, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в РС;

5) Пользователь РС – физическое или юридическое лицо, правомерно владеющее закрытым ключом ЭЦП, обладающее правом на ее использование на электронном документе;

6) Доверяющая сторона – информационные системы, использующие полученные в Центре сертификации сведения о РС для проверки принадлежности электронной цифровой подписи владельцу РС;

7) Сервер метки времени – служба для постановки метки времени на электронный документ. Служба работает на основе протокола меток времени - Time-Stamp Protocol (TSP);

8) Сервер проверки статуса РС – служба определения статуса РС. Служба работает на основе протокола Online Certificate Status Protocol (OCSP).

Глава 2. Организационно-технические и административные меры обеспечения безопасности

6. Для обеспечения безопасности УЦ применяются организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

7. Защита информации от несанкционированного доступа осуществляется на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

8. Защита информации от несанкционированного доступа предусматривает контроль эффективности средств защиты от несанкционированного доступа. ПИТБ производит проверку на соответствие требованиям ИБ в соответствии с «Инструкцией по проведению проверок информационных систем на соответствие требованиям информационной безопасности».

9. Контроль и управление доступом в помещения УЦ осуществляется согласно Правилам о критичных зонах.

10. Центр Сертификации, обрабатывающий запросы участников УЦ, расположен в специализированном для размещения серверов и оборудования помещении, контроль и предоставление доступа к которому осуществляется согласно «Правилам о критичных зонах». Доступ в центр обработки данных предоставляется лицам, перечень которых утверждается руководителем подразделения по информационным технологиям по согласованию с подразделением по информационной безопасности. Банк ведёт журнал системы контроля и управления доступом в центр обработки данных, который хранится не менее 1 (одного) года.

11. Режимные помещения информационных технологий Центра Сертификации находятся в нежилом помещении, оборудованы источниками бесперебойного питания, средствами вентиляции, кондиционирования воздуха, а так же средствами пожаротушения и контроля влажности согласно «Правилам о критичных зонах», обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха в соответствии с нормами, устанавливаемыми законодательством Республики Казахстан.

12. Оборудование серверного помещения должно быть соединено с главным электродом системы заземления здания кондуитом размером не менее 1,5 см, высота потолка серверного помещения должна составлять не менее 2,44 метра. Ответственными работниками ведётся прошнурованный журнал проводимых работ в серверном помещении.

13. Процесс приёма работников, в том числе проверка биографии и обучение новых работников, осуществляется в соответствии с «Правилами подбора, приема и адаптации персонала».

14. В случае переноса средств УЦ на новое оборудования или программное обеспечение, персонал Центра Сертификации проходит курс обучения работе с новыми средствами.

15. В исключительных случаях, когда для выполнения работ по настройке или поддержке оборудования и информационной системы УЦ требуются услуги независимых подрядчиков, специалисты подрядчиков проводят работы только под наблюдением и с разрешения работников УЦ в рамках «Правил разграничения прав доступа к электронным информационным ресурсам»

16. Деятельность работников УЦ регламентирована внутренними нормативными документами Банка, в их числе:

1) «Политика информационной безопасности Удостоверяющего центра»;
2) «Положение об Удостоверяющем центре»;
3) «Политика применения регистрационных свидетельств Удостоверяющего центра»;
4) «Инструкция по сопровождению, администрированию, выпуску регистрационных свидетельств в нештатных-кризисных ситуациях»;
5) «Инструкция по установке и настройке программного обеспечения удостоверяющего центра»;
6) «Инструкция о резервном копировании информационных ресурсов Удостоверяющего центра»;
7) «Инструкция по закреплению функций и полномочий администратора сервера Удостоверяющего центра»;
8) «Правила организации процедуры аутентификации»;
9) «Правила разграничения прав доступа к электронным информационным ресурсам»;
10) «Правила обеспечения конфиденциальности информации»;
11) «Правила безопасного использования информационных ресурсов»;
12) «Инструкция по проведению проверок информационных систем на соответствие требованиям информационной безопасности»;
13) «Инструкция по управлению уязвимостями информационных систем»;
14) «Инструкция по управлению инцидентами информационной безопасности»;
15) «Инструкция по управлению доступами на межсетевых экранах»;
16) «Правила организации антивирусной защиты информационных систем»;
17) «Стандарт информационных систем Банка»;
18) «Инструкция по управлению запросами на обслуживание и ИТ-инцидентами»;
19) «Регламент приема систем/функционала в промышленную эксплуатацию/вывода из промышленной эксплуатации».

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

18. Программно-аппаратный комплекс УЦ, помимо установленных «Стандартом информационных систем Банка», регистрирует следующие виды событий аудита:

- системные события общесистемного программного обеспечения;
- принятие запроса на выпуск РС;
- выпуск РС;
- помещение запроса на РС;
- принятие запроса на РС;
- отклонение запроса на РС;
- выпуск/перевыпуск списка отозванных РС;
- невыполнение внутренней операции программной компоненты.
- формирование закрытого ключа РС облачном компоненте УЦ;
- использование закрытого ключа РС облачной ЭЦП;
- удаление (стирание) закрытого ключа РС облачной ЭЦП.

18-1. Срок хранения протоколов работы составляет не менее одного года с даты истечения срока действия РС. При протоколировании действий записывается следующая информация:

– идентификатор владельца;
– дата, время;
– событие.

18-2. Протоколы событий ежедневно преобразуется в хэш, и данные хэш хранятся в цепочке событий блокчейн. Применяемый для этого блокчейн доступен в Интернете.

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

20. Журналы аудита постоянно автоматически анализируются с помощью системы мониторинга и анализа логов, с целью обнаружения уязвимостей и нарушений в работе программного и аппаратного обеспечения Центра Сертификации. Хранение и защита журналов осуществляется согласно «Стандарту информационных систем Банка».

21. В процессе анализа журналов аудита проводится расследование всех значительных нарушений работы, и принимаются адекватные меры реагирования, согласно «Инструкции по управлению запросами на обслуживание и ИТ-инцидентами» и «Инструкции по управлению инцидентами информационной безопасности».

22. УЦ ведет электронный архив:
- журналов аудита в соответствии с пунктом 20 Правил;
- заявлений на выдачу и отзыв РС;
- копии документов, удостоверяющих личность и данных с них;
- РС пользователей УЦ, срок действия которых истек;
- отозванных РС пользователей УЦ;
- списков отозванных РС УЦ;
- протоколов работы программного обеспечения УЦ;
- прочих документов, хранение которых осуществляется согласно Перечню.

23. УЦ обеспечивает ведение архива и хранение архивных документов в соответствии с законодательством Республики Казахстан, при этом обеспечивается постоянное хранение архива:
- РС ключей электронных цифровых подписей;
- документов о создании и аннулировании электронной цифровой подписи (заявления, РС, уведомления и другие документы);
- журналов (перечни, реестры) учета выданных регистрационных свидетельств, подтверждающих соответствие электронной цифровой подписи.

24. Доступ к архиву имеют только уполномоченные работники Центра Сертификации, согласно «Инструкции по закреплению функций и полномочий администратора сервера Удостоверяющего центра».

25. Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению в соответствии с Перечнем, осуществляется работниками УЦ, согласно «Правилам обеспечения конфиденциальности информации».

26. За 10 рабочих дней до окончания срока действия закрытого ключа уполномоченного лица Центра Сертификации, администратор ПО УЦ производит формирование нового закрытого ключа и РС уполномоченного лица Центра Сертификации и публикует его в соответствующий раздел хранилища РС, аналогично первичной генерации, согласно «Инструкции по установке и настройке программного обеспечения удостоверяющего центра».

27. По окончании действия закрытого ключа Центра Сертификации, носители ключевой информации с закрытым ключом и его копиями уничтожаются по акту ответственными работниками ПИТБ под контролем руководителя ПИТБ, способами, описанными в «Правилах обеспечения конфиденциальности информации».

28. Исключен.

29. Для предотвращения потери, данные Центра Сертификации (хранилище выпущенных РС, ключи Центра Сертификации) архивируются и помещаются в специально предназначенные для этих целей хранилища. Архивирование хранилища выпущенных РС и СОРС осуществляется автоматически не реже одного раза в сутки. Резервное копирование осуществляется не реже 1 раза в месяц, дублирование ключей между основным и резервным HSM происходит 1 раз в сутки.

30. В случае повреждения оборудования, программных и/или аппаратных сбоев производится регистрация инцидента и действия по его решению и минимизации последствий, а также фиксируются данные по недопущению его в будущем, согласно «Инструкции по сопровождению, администрированию, выпуску регистрационных свидетельств в нештатных-кризисных ситуациях».

31. В случае технических сбоев в работе интернет-ресурса УЦ отзыв РС приостанавливается до восстановления работы интернет-ресурса УЦ.

32. Закрытые ключи РС облачного компонента УЦ генерируются строго внутри HSM. Закрытый ключ не извлекается из HSM в открытом виде. При этом HSM:

1) соответствует не ниже 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.

3) соответствует нормам эффективности защиты и методикам оценки защищенности информации и технических средств согласно требованиям действующего законодательства Республики Казахстан.

33. Исключен.

34. Исключен.

35. Исключен.

36. Ключи ЭЦП формируются и используются криптографическим преобразованием по алгоритму ГОСТ 34.310-2004:

- закрытый ключ – 256 бит;
- открытый ключ – 512 бит.

37. Цели использования ключа (порядок заполнения поля key usage РС x.509v3) заполняются в соответствии с Политикой.

38. Все действия с носителями ключевой информации должны осуществляться строго в соответствии с инструкциями по их эксплуатации, предоставленных поставщиком носителей ключевой информации, и требованиями безопасности, описанными в документах, указанных в пункте 16 Правил.

39. Срок хранения отозванных регистрационных свидетельств в регистре регистрационных свидетельств составляет не менее 5 (пяти) лет со дня отзыва. По истечении срока хранения, отозванные РС в электронном виде поступают на архивное хранение в соответствии с Перечнем.

40. Исключен.

41. Документы (заявления об изготовлении ЭЦП, регистрационного свидетельства, заявления и уведомления об отзыве регистрационного свидетельства, акты уничтожения закрытого ключа ЭЦП и другие документы) о создании и отзыве ЭЦП хранятся постоянно согласно Перечню.

42. Резервное копирование закрытого ключа Центра Сертификации производится ответственными работниками УЦ после его генерации в соответствии с эксплуатационной документацией средства криптографической защиты информации, предоставленной поставщиком средства криптографической защиты информации, по схеме n из m, которая подразумевает разделение секрета на N частей, из которых для расшифрования достаточно только M частей секрета. Каждой частью секрета владеет отдельный человек. Резервная копия закрытого ключа Центра Сертификации хранится отдельно от криптографического модуля в зашифрованном архиве на носителе информации, хранящимся в закрытом физическом хранилище.

43. Запись закрытого ключа на носитель ключевой информации и уничтожение закрытых ключей с истекши сроком действия производится в соответствии с эксплуатационной документацией. Архивное хранение закрытых ключей, которые выпускаются не облачным путем, не допускается.

44. Исключен.

45. Предоставление открытого ключа Центра Сертификации реализовано посредством публикации его РС в хранилище и на интернет-ресурсе http://crt.eubank.kz/EubankCA.crt.

46. Безопасность РС Центра Сертификации реализована путем предоставления информации о серийном номере РС и его хеш-значения, с предоставлением доверяющим сторонам возможности его проверки на интернет-ресурсе https://eubank.kz/data-of-the-registration-certificate-of-the-certification-center/».

47. В случае смены ключей подписи Центра Сертификации и выпуска нового РС Центра Сертификации, его распространение может производиться с использованием механизма кросс-сертификации.

48. Исключен.

49. Компьютеры, работающие в УЦ, удовлетворяют следующим требованиям:

- компьютеры для подписи РС изолированы для неавторизованного доступа;
- операционные системы поддерживаются на высоком уровне защиты, при регулярном применении всех рекомендованных поставщиком операционной системы и соответствующих пакетов защиты, в том числе антивирусов;
- мониторинг осуществляется для обнаружения несанкционированных программных изменений;
- количество запущенных системных служб сведено к минимуму.

50. Компьютеры пользователей РС и доверяющих сторон должны удовлетворять следующим требованиям:

- использование лицензионного программного обеспечения;
- операционные системы поддерживаются на высоком уровне защиты, при регулярном применении всех рекомендованных поставщиком операционной системы и соответствующих пакетов защиты, в том числе антивирусов и межсетевых экранов;
- в случаях совместного использования компьютера несколькими пользователями, применяется разграничение доступа, основанное на использовании различных учётных записей со сложными паролями;
- на компьютере отсутствуют средства криптографической защиты информации, отличные от определенных в Правилах.

51. Безопасность Центра Сертификации обеспечивается межсетевыми экранами и прочими программно-аппаратными средствами информационной безопасности.

Глава 3. Процедура первичной регистрации

52. Первичная регистрация заявителя – это процесс, в результате которого физическое, либо юридическое лицо впервые сообщает о себе УЦ, до того, как будут выпущен РС для данного физического, либо юридического лица. Конечным результатом данного процесса (если он успешен), является выпуск РС для открытого ключа заявителя и выдача ему РС и/или помещение его в хранилище РС.

53. Заявление на выдачу РС имеют право подавать физические и юридические лица, резиденты РК.

54. Лицо, желающее пройти процедуру регистрации, должно подтвердить свое полное и безоговорочное присоединение к Правилам и Политике, а также дать согласие на:

- видеосъемка/фотографирование себя и своих документов, а также использование данных изображений в целях получения услуг в рамках Правил;
- сбор, обработку персональных и биометрических данных в целях получения выдачи и отзыва регистрационного свидетельства УЦ.

54-1. Владелец может получить РС:

1) удаленно, в таком случае РС хранится в УЦ. Владелец дает согласие на хранение закрытого ключа ЭЦП в облачном компоненте УЦ;

2) нарочно в центре регистрации УЦ, в таком случае РС хранится у владельца в форме электронного документа путем записи регистрационных свидетельств на носитель информации.

54-2. В случае прохождения биометрической аутентификации УЦ обеспечивает хранение биометрических данных владельца не менее 5 (пять) лет.

55. Для получения РС удаленно посредством интернет-ресурсов УЦ физическое лицо проходит аутентификацию с использованием многофакторной аутентификации, в котором одним из методов является биометрическая аутентификация, фотографирует документ, удостоверяющий личность физического лица, и подписывает ОТР заявление на выдачу регистрационных свидетельств от физического лица по форме, согласно приложению №1 к настоящим Правилам, а также заявление на сбор и обработку персональных данных. В качестве секретных значений участвуют пароль, заданный владельцем, который в УЦ не хранится. УЦ для проверки пароля от закрытого ключа владельца хранит

хэш пароля в HSM. При передаче пароля от владельца (браузер, мобильное приложение) в HSM производится в зашифрованном виде, при этом шифрование пароля производится на стороне владельца, в персональном компьютере или смартфоне. Восстановление пароля от закрытого ключа ЭЦП в облачном компоненте ЭЦП не осуществляется.

56. При физическом обращении в УЦ для получения регистрационных свидетельств юридическое лицо (либо его представитель по доверенности) нарочно предоставляет в центр регистрации следующие документы:

1) заявление на выдачу регистрационных свидетельств от юридического лица по форме, согласно приложению №2 к настоящим Правилам;

2) копию документа, удостоверяющего личность представителя юридического лица;

3) справку либо свидетельство о государственной регистрации (перерегистрации) юридического лица заявителя в качестве юридического лица (либо копию, удостоверенную нотариально в случае непредставления оригиналов) – для юридического лица;

4) доверенность на представителя юридического лица, с указанием полномочия представлять документы на выдачу регистрационных свидетельств удостоверяющего центра и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью.

57. Исключен.

58. УЦ обрабатывает заявления на выдачу РС заявителей в течение 1 (одного) рабочего дня со дня подачи заявления.

59. УЦ оставляет за собой право осуществлять проверку сведений, указанных в заявлении на выдачу РС, а также требовать от заявителя представления дополнительных документов, подтверждающих сведения, указанные в заявлении.

60. В регистрации РС может быть отказано в случае, если:

- заявителем не представлена (либо не полностью представлена) необходимая информация;
- заявителем представлена недостоверная информация;
- вступило в законную силу решение суда;
- лицо не достигло шестнадцатилетнего возраста.

61. В случае отказа в регистрации РС, производится уведомление заявителя с помощью одного из доступных каналов связи (электронная почта, телефонный звонок, sms, интернет-ресурс, push-уведомление) не позднее 1 (одного) рабочего дня со дня подачи заявления. При устранении заявителем причин отказа в оказании услуги, заявитель подает повторное заявление для получения услуги по выдаче и отзыву РС в порядке, установленном в Правилах.

62. Исключен.

63. Исключен.

64. Исключен.

65. Исключен.

66. Следующие действия владельца РС означают признание РС:

- получение регистрационного свидетельства;
- отсутствие у владельца мотивированных возражений (претензий) по поводу содержания РС.

Глава 4. Процедура отзыва регистрационных свидетельств

67. Замена ключей до истечения срока действия РС может быть выполнена при предоставлении запроса, об отзыве РС, с дальнейшим прохождением процедуры первичной регистрации, описанной в Главе 3.

68. Заявление на отзыв РС может подавать его владелец, либо его представитель по доверенности.

69. РС отзываются на основании предоставления в отделении Банка владельцем регистрационного свидетельства – физическим лицом (либо его представителем по доверенности) следующих документов:

1) заявление на отзыв регистрационного свидетельства от физического лица по форме, согласно приложению №3 к настоящим Правилам;

2) копию документа, удостоверяющего личность физического лица;

3) доверенность на представителя физического лица, удостоверенную нотариально с указанием полномочия представлять документы на отзыв регистрационных свидетельств

удостоверяющего центра и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью – при представлении интересов физического лица третьим лицом.

69-1. После сбора необходимых документов, работник отделения Банка направляет запрос посредством Naumen в Центр регистрации для отзыва РС.

70. РС отзываются на основании предоставления в отделении Банка владельцем регистрационного свидетельства – юридическим лицом (либо его представителем по доверенности) следующих документов:

1) заявление на отзыв регистрационного свидетельства от юридического лица по форме, согласно приложению №4 к настоящим Правилам;

2) копию документа, удостоверяющего личность представителя юридического лица;

3) доверенность на представителя юридического лица, с указанием полномочия представлять документы на отзыв регистрационных свидетельств удостоверяющего центра и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью.

70-1. После сбора необходимых документов, работник отделения Банка направляет запрос посредством Naumen в Центр регистрации для отзыва РС.

71. УЦ отзывает РС в течение 1 (одного) рабочего дня с момента принятия УЦ заявления, полученного от владельца РС (либо его представителя по доверенности) на отзыв РС.

72. В случае отзыва регистрационных свидетельств удостоверяющий центр оповещает об этом владельца регистрационного свидетельства путем незамедлительного внесения в регистр регистрационных свидетельств соответствующей информации с указанием даты и времени отзыва регистрационных свидетельств, что является официальным уведомлением участников УЦ об отзыве РС.

73. Удостоверяющий центр публикует на интернет-ресурсе http://crl.eubank.kz/GOST.crl сведения об отозванных регистрационных свидетельствах, их серийные номера, дату и причину отзыва в СОРС.

74. СОРС обновляется по мере поступления запросов на смену статуса Регистрационного свидетельства. Отозванные РС с истекшим сроком действия, удаляются из СОРС.

75. Владелец Регистрационного свидетельства самостоятельно проверяет факт отзыва Регистрационного свидетельства. Проверка факта отзыва может осуществляться с использованием СОРС.

76. Заявление на отзыв РС следует подавать в течение минимально возможного времени после появления такой необходимости (например, в случае компрометации закрытого ключа). В случае выявления факта компрометации закрытых ключей электронной подписи владельцев регистрационных свидетельств, УЦ незамедлительно публикует на своем интернет-ресурсе информацию о данном факте и принятых мерах по минимизации нанесенного ущерба.

77. УЦ может отозвать РС и осуществить публикацию его в СОРС в следующих случаях:

1. по требованию владельца регистрационного свидетельства либо его представителя;
2. при установлении факта представления недостоверных сведений либо неполного пакета документов при получении регистрационного свидетельства;
3. смерти владельца регистрационного свидетельства;
4. изменения фамилии, имени или отчества (если оно указано в документе, удостоверяющем личность) владельца регистрационного свидетельства;
5. смены наименования, реорганизации, ликвидации юридического лица – владельца регистрационного свидетельства, смены руководителя юридического лица;
6. предусмотренных соглашением между удостоверяющим центром и владельцем регистрационного свидетельства;
7. по вступившему в законную силу решению суда.

77-1. Удостоверяющий центр производит отзыв регистрационного свидетельства без заявления от заявителя при получении достоверных сведений о наступлении одного из случаев, указанных в подпунктах 2,3,4,5,6,7 пункта 77 настоящих Правил.

78. При выявлении нарушений в функционировании УЦ, разрабатывается план действий по устранению выявленных нарушений в соответствии с «Инструкцией по управлению инцидентами информационной безопасности». Если выявленные нарушения привели к выдаче РС, нарушающих безопасность УЦ, эти РС будут немедленно отозваны. В случае выявления нарушений в функционировании, УЦ сообщит о действиях, которые необходимо предпринять для восстановления

надлежащего функционирования. Если в процессе изготовления РС Центр Сертификации функционировал с нарушениями, выпущенные в это время РС должны быть отозваны.

Глава 5. Операционные требования к жизненному циклу РС

79. Начало периода действия РС Центра Сертификации исчисляется с даты и времени его генерации. Срок действия корневого РС УЦ составляет 20 (двадцать) лет.

80. Срок действия пользовательского РС составляет от 3 месяцев до 3 лет. Начало периода действия закрытого ключа владельца РС исчисляется с даты и времени начала действия соответствующего РС владельца РС.

80-1. УЦ предоставляет владельцу закрытого ключа облачного компонента ЭЦП доступ к информации о всех подписанных электронных документах через личный кабинет УЦ. Срок хранения информации обо всех подписанных электронных документах составляет не менее одного года после истечения срока действия регистрационного свидетельства владельца. Подписание электронных документов осуществляется в памяти HSM путем передачи подписываемого файла или его хэш в HSM.

81. Закрытый ключ Центра Сертификации используется для формирования ЭЦП, РС, открытых ключей пользователей и списков отозванных РС.

82. Закрытые ключи пользователей УЦ используются для формирования ЭЦП электронных документов.

83. Закрытый ключ используется для формирования электронной цифровой подписи.

84. РС используется для подтверждения подлинности электронной цифровой подписи. Проверка производится путем предоставления сведений о статусе выданных РС и РС уполномоченных лиц Центра сертификации участникам УЦ, согласно Главе 6. Каждый РС, выданный УЦ, содержит ссылку на списки отозванных РС.

85. После начала использования РС, оно считается признанным владельцем РС.

86. Пользователь РС должен использовать РС строго в соответствии с указанными в нем сведениями и Правилами. Получение дополнительных сведений и гарантий, помимо сведений, указанных в РС, осуществляется участниками УЦ самостоятельно.

87. Владелец РС должен самостоятельно осуществлять проверку статуса РС.

88. В случае компрометации ключей уполномоченных лиц Центра Сертификации, УЦ незамедлительно оповещает участников УЦ любыми из доступных способов.

89. Владельцы РС могут быть участниками единого пространства доверия с владельцами РС, выданными другими Центрами Сертификации в тех случаях, когда между Центрами Сертификации заключено соответствующее соглашение и приняты необходимые организационно-технические меры.

90. Исключен.

91. Список отозванных РС предоставляется владельцам РС в электронной форме в формате, определенном RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile). Список заверяется ЭЦП Центра Сертификации.

92. Участник УЦ может закончить использование услуг УЦ путем отзыва своего РС или отказа от смены пар ключей после окончания их срока действия.

93. Процедура проверки ЭЦП электронного документа включает в себя проверку действительности использования РС на момент подписания, проверку подлинности ЭЦП и проверку соответствия использования ЭЦП сведениям в РС.

Глава 6. Порядок подтверждения принадлежности и действительности открытого ключа ЭЦП УЦ

94. Подтверждение принадлежности и действительности открытого ключа ЭЦП УЦ осуществляется участником УЦ или информационной системой УЦ при обмене электронными документами между участниками УЦ.

95. Участник УЦ при получении электронного документа, содержащего РС подписывающей стороны, осуществляет его проверку на подтверждение принадлежности и действительности открытого ключа ЭЦП путем:

1) проверки регистрационных свидетельств подписывающей стороны;
2) проверки ЭЦП в электронном документе.

96. Проверка регистрационных свидетельств подписывающей стороны осуществляется путем выполнения следующих проверок с использованием СКЗИ УЦ:

1) проверка построения корректной цепочки от проверяемых регистрационных свидетельств до доверенного корневого регистрационного свидетельства УЦ, с учетом промежуточных регистрационных свидетельств УЦ;

2) проверка срока действия регистрационных свидетельств. Проверка сроков действия от проверяемых регистрационных свидетельств до доверенного корневого регистрационного свидетельства УЦ, с учетом промежуточных регистрационных свидетельств УЦ;

3) проверка регистрационных свидетельств на отзыв. Проверка регистрационных свидетельств на отзыв подписывающей стороны осуществляется одним из методов:

- на основе СОРС УЦ. Данный метод проверки подтверждает, отозваны ли проверяемые РС на момент начала срока действия СОРС УЦ;
- онлайн проверка регистрационных свидетельств на отзыв, основанная на протоколе OCSP. Данный метод проверки подтверждает, отозвано ли проверяемые РС на момент отправки запроса (текущее время);

4) проверка области использования ключа. Проверка заключается в определении наличия требуемых значений поля регистрационных свидетельств «использование ключа» (KeyUsage). Если поле «использование ключа» содержит значения «Цифровая подпись» и «Неотрекаемость», то эти РС используется для ЭЦП;

5) проверка номера политики регистрационных свидетельств и разрешенных способах их использования. Если политика проверяемых регистрационных свидетельств предусматривает ограничение их использования (только в одной системе), то данные РС и соответствующий закрытый ключ не используются в других системах;

6) проверка метки времени. Доказательством подписания документа в указанный момент времени является метки времени, полученная в УЦ и содержащая время подписания документа. Данная проверка производится для электронных документов долговременного хранения и формируется в момент подписания документа;

7) исключен;

8) проверка подтверждения принадлежности и действительности открытого ключа ЭЦП в электронном документе производится с использованием СКЗИ УЦ путем использования открытого ключа, который содержится в регистрационном свидетельстве подписывающей стороны. Техническая реализация проверки ЭЦП возлагается на владельца информационной системы;

9) в случае если ЭЦП или регистрационное свидетельство не соответствует требованиям хотя бы одного из критериев вышеописанных проверок, за исключением проверки метки времени, то ЭЦП или регистрационное свидетельство считается недействительным;

10) техническая реализация проверки принадлежности и действительности открытого ключа ЭЦП и регистрационного свидетельства возлагается на информационную систему, путем использования высокоуровневых функций разработки с применением СКЗИ УЦ.

Глава 7. Конфиденциальность

97. Участники УЦ признают, что информация, доступ к которой ограничивается в соответствии с законодательством Республики Казахстан и представляющая собой коммерческую, служебную, банковскую, личную и иную охраняемую законом тайну, рассматривается в качестве конфиденциальной информации.

98. Участники УЦ, признают, что содержимое РС, информация об их отзыве или иная информация о статусе РС, публичная часть хранилища и содержащаяся в них информация не рассматриваются в качестве конфиденциальной информации. Информация, не перечисленная в пункте 102 Правил, не рассматривается как конфиденциальная, если иное не предусмотрено действующим законодательством Республики Казахстан.

99. Участники УЦ обязаны хранить в тайне информацию, рассматриваемую в качестве конфиденциальной.

100. УЦ обеспечивает защиту сведений о владельцах РС и раскрывает их только в случаях, предусмотренных законодательством Республики Казахстан.

101. УЦ в своей деятельности руководствуется действующим законодательством Республики Казахстан по вопросам защиты персональных данных. В частности, УЦ не разглашает информацию, идентифицирующую заявителей на выпуск РС, за исключением информации, перечисленной в пункте 103 Правил.

102. Информация, рассматриваемая как конфиденциальная указана в Реестре конфиденциальных данных.

103. Информация, которая не считается конфиденциальной:

- списки отозванных РС;
- статус РС участника УЦ;
- открытый ключ РС участника УЦ.

104. Статистика относительно выдачи и отзыва РС не содержит никакой персональной информации и не считается конфиденциальной.

Глава 8. Обязанности

105. Участник УЦ обязуется:

1) исключен;

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

3) соблюдать и принимать установленные УЦ меры по охране конфиденциальной информации, переданной (полученной) на материальных носителях:

- хранение и использование конфиденциальной информации должно осуществляться участником УЦ в местах, обеспечивающих физическую сохранность конфиденциальной информации и авторизацию доступа;
- на устройствах, являющихся материальным носителем ключевой информации, должны быть установлены пароли, с целью обеспечить сохранность данной информации и исключить доступ к конфиденциальной информации всех лиц, кроме лица, уполномоченного владеть доступом к носителю;
- извлечение конфиденциальной информации за пределы мест ее хранения/использования не допускается;
- во время работы (выполнения действий, операций) с конфиденциальной информацией должна быть исключена возможность ознакомления с нею лиц, не уполномоченных на такое ознакомление (доступ);
- копирование или иное воспроизведение конфиденциальной информации и/или ее материальных носителей, допускается лишь с письменного согласия УЦ. При этом неудачные или ненужные копии и иные результаты воспроизведения конфиденциальной информации (ее материальных носителей) подлежат обязательному уничтожению с помощью специальных механических устройств или вручную. В отношении копий и иных результатов воспроизведения конфиденциальной информации и/или ее материальных носителей участник УЦ обязан придерживаться тех же мер защиты, как и в отношении оригиналов;
- при предоставлении конфиденциальной информации в установленных законодательством случаях органу государственной власти, иным государственным органам, органам местного самоуправления одновременно с таким предоставлением уведомить в письменной форме об этом УЦ.

106. В случае разглашения Владельцем РС, Пользователем РС конфиденциальной информации, как по вине последних, так и без таковой, УЦ не несет ответственности за негативные последствия, обусловленные разглашением конфиденциальной информации.

107. Центр Сертификации ответственен за изготовление РС и последующее управление ими в соответствии с настоящими Правилами, в частности, он:

- обрабатывает запросы на выдачу РС и издает новые РС, в соответствии с запрашиваемой областью применения;
- подтверждает запросы на выдачу РС от участников УЦ, запрашивающих РС согласно процедурам, описанным в Правилах;
- издает РС на основе запросов от аутентифицированных заявителей;
- посылает уведомление о статусе выпущенных РС по запросам заявителей;
- публикует информацию о выпущенных РС в хранилище РС;

- публикует корневое РС Центра Сертификации в хранилище РС;
- обрабатывает запросы на отзыв РС;
- подтверждает запросы на отзыв РС от заявителей согласно процедурам, описанным в данном документе;
- выпускает СОРС;
- публикует информацию об отозванных РС;
- осуществляет хранение закрытых ключей владельца регистрационного свидетельства на стороне УЦ в HSM.

108. Центр регистрации отвечает за проведение процедур идентификации и аутентификации, в частности, они:
- проверяют информацию, предоставленную заявителем при регистрации в УЦ, на полноту, достоверность и точность;
- передают запросы на выпуск РС по защищенному каналу в Центр Сертификации;
- осуществляют консультацию заявителей на предмет прохождения процедур идентификации и аутентификации в УЦ.

109. Направляя запрос на выдачу РС, заявители соглашаются:
- принять условия и следовать процедурам, описанным в Правилах;
- предоставить достоверную и точную информацию при регистрации в УЦ;
- при изменении учетных данных, предоставленных в документах при регистрации, незамедлительно направить заявку на отзыв РС;
- использовать сервисы УЦ в соответствии с Правилами;
- применять для формирования ЭЦП только действующий закрытый ключ ЭЦП, соответствующий открытому ключу ЭЦП, указанному в РС участника УЦ;
- применять секретные ключи и соответствующие им РС в соответствии с областью применения и политиками, указанными в РС;
- обеспечивать сохранность носителя ключевой информации и не допускать неправомерного распространения информации о своем закрытом ключе;
- не использовать секретные ключи и соответствующие им РС по истечении срока их действия;
- не использовать секретные ключи и соответствующие им РС в случае их отзыва;
- немедленно направить в УЦ запрос на отзыв РС в случае, если секретный ключ потерян или есть основания полагать, что информация о секретном ключе стала доступной третьим лицам.

110. При использовании РС, выданного УЦ, доверяющие стороны соглашаются:
- принять условия и следовать процедурам, описанным в Правилах;
- проверить сроки действия, ЭЦП и политики РС;
- не использовать секретные ключи и соответствующие им РС по истечении срока их действия;
- проверить статус РС, используя списки отозванных РС;
- не использовать секретные ключи и соответствующие им РС в случае их отзыва;
- использовать РС в соответствии с Правилами, Политикой и действующим законодательством.

111. РС не может быть использован до наступления срока действия или после истечения срока действия, в случае неверной ЭЦП и/или после приостановления/отзыва.

Глава 9. Ответственность

112. Работники УЦ несут ответственность за свои действия в соответствии с законодательством Республики Казахстан.

113. УЦ не несет ответственности за последствия, возникшие в результате нарушения пользователями и/или доверяющими сторонами положений Правил и/или действующего законодательства.

114. УЦ гарантирует обработку запросов на выдачу РС согласно процедурам, описанным в Правилах.

115. УЦ гарантирует обработку запросов на отзыв согласно процедурам, описанным в Правилах.

116. УЦ гарантирует отсутствие в РС умышленных искажений данных участников УЦ.
117. Претензии к УЦ ограничиваются указанием на несоответствие ее действий Правилам.
118. УЦ не обязан возмещать расходы, связанные с:

- представлением участниками УЦ ошибочной, вводящей в заблуждение или заведомо ложной информации при регистрации (в заявлении на выпуск РС);
- непринятием участниками УЦ мер защиты собственного закрытого ключа, приведшими к его компрометации, утере, разглашению, изменению или несанкционированному использованию;
- непринятием участниками УЦ мер по проверке РС с целью определения его статуса (отозван/действителен), области применения (политики) и сроков действия;
- использованием участниками УЦ в составе своего отличительного имени названий, нарушающих права интеллектуальной собственности третьих лиц.

Раздел 3. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

119. Исключен.
120. Официальным уведомлением участников УЦ об утверждении изменений Правил является публикация на интернет-ресурсе https://eubank.kz/rules-of-operation-of-the-certification-center/».
121. УЦ оставляет за собой право без предварительного уведомления вносить изменения и дополнения в Правила, включая, но не ограничиваясь исправлением опечаток, изменением адресов ссылок и контактной информации.
122. Правила должны приводиться в соответствие в связи с возникающими внутренними и внешними изменениями и в обязательном порядке изменяться, уточняться и совершенствоваться, для поддержания эффективности управления информационной безопасностью УЦ.
123. Все изменения, вносимые в Правила, вступают в силу и становятся обязательными к исполнению всеми участниками УЦ немедленно после их публикации на интернет-ресурсе https://eubank.kz/rules-of-operation-of-the-certification-center/».
124. В случае несогласия с изменениями (дополнениями) Правил Владелец РС обязан отозвать РС в порядке, предусмотренном в Главе 5 Правил.
125. В случае если часть положений Правил будет признана неосуществимой судом или уполномоченным государственным органом, остальная ее часть сохраняет силу.
126. С момента прекращения действия Правил участники УЦ остаются связанными его условиями по всем РС до момента истечения периода их действия.
127. Применимым правом для разрешения споров, предметом которых являются разногласия по существу Правил, является законодательство Республики Казахстан.
128. Вопросы, не урегулированные Правилами, разрешаются в соответствии с законодательством Республики Казахстан и ВНД.

Директор службы ИТ-безопасности
Рустамов Э.А.

ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ

№	Номер приложения	Наименование приложения
1.	Приложение №1	Форма заявления на выдачу регистрационных свидетельств от физического лица
2.	Приложение №2	Форма заявления на выдачу регистрационных свидетельств от юридического лица
3.	Приложение №3	Заявление на отзыв регистрационных свидетельств от физического лица
4.	Приложение №4	Заявление на отзыв регистрационных свидетельств от юридического лица
5.	Приложение №5	SIPOC

ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

№ п/п	Номер протокола	Дата протокола	Дата вступления в силу	Инициатор изменений
1.	149-08	26.10.2020	16.11.2020	Служба ИТ безопасности
2.	165-13	23.11.2020	22.01.2021	Служба ИТ безопасности
3.	155-05	04.09.2023	12.09.2023	Служба ИТ безопасности