Утверждено
Протоколом Правления (Решение)
№ 3-0721-04 от 21.07.2022 г.

Регламент
деятельности удостоверяющего центра
АО «Банк ЦентрКредит»

Содержание

Глава 1. Введение

Раздел 1.1. Общие положения

1. Настоящий Регламент деятельности удостоверяющего центра АО «Банк ЦентрКредит» (далее – Регламент) разработан в соответствии с требованиями нормативных правовых актов Республики Казахстан по вопросам электронного документа и электронной цифровой подписи, в целях обеспечения функционирования удостоверяющего центра АО «Банк ЦентрКредит» (далее – Удостоверяющий центр/Банк) и определяет порядок его функционирования.
2. Настоящий 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).
3. Настоящий Регламент определяет меры, реализуемые Удостоверяющим центром при обеспечении набора сервисов, который определен Политикой применения регистрационных свидетельств удостоверяющего центра АО «Банк ЦентрКредит» (далее – Политика регистрационных свидетельств) и включает в себя, но не ограничивается выпуском, управлением и отзывом регистрационных свидетельств.
4. Политика регистрационных свидетельств определяет виды регистрационных свидетельств, выпускаемых Удостоверяющим центром, определяет 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. Настоящий Регламент, в отличие от Политики регистрационных свидетельств, определяет порядок и процедуры, в соответствии с которыми:
1) выполняются функции (работают сервисы) Удостоверяющего центра;
2) обеспечивается безопасность и управление ядром инфраструктуры открытых ключей.
6. С момента подписания участником информационной системы, использующей сервисы Удостоверяющего центра, заявления на выпуск регистрационного свидетельства, для участника становятся обязательными к выполнению применимые к нему требования той Политики регистрационных свидетельств, ссылка на которую содержатся в заявлении, и настоящего Регламента.
7. Настоящий Регламент также определяет процедуры проверки, связанные с выпуском и дальнейшим обслуживанием тех видов регистрационных свидетельств, которые выпускает Удостоверяющий центр, в соответствии с Политикой регистрационных свидетельств.
8. Исчерпывающий перечень видов регистрационных свидетельств, выпускаемых Удостоверяющим центром, с указанием идентифицирующих их признаков (профилей) приведен в нижеследующей таблице.

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

Раздел 1.2. Наименование и атрибуты документа

9. Документ именуется «Регламент деятельности удостоверяющего центра АО «Банк ЦентрКредит»», как этого требует правовой акт по вопросам аккредитации удостоверяющих

центров, изданный уполномоченным органом в сфере обеспечения информационной безопасности[1].
10. Редакция документа 1.0.0.
11. Регламент в настоящей редакции введен в действие протокольным решением Правления Банка от 21.07.2022 года № 3-0721-04.
12. Действующая редакция Регламента публикуется на официальном информационном ресурсе Банка в сети Интернет.
13. Настоящий Регламент зарегистрирован в дереве международных объектных идентификаторов с присвоением объектного идентификатора.

Раздел 1.3. Участники инфраструктуры открытых ключей Банка

14. Удостоверяющий центр – структурное подразделение Банка, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства[2].
15. Центры регистрации Удостоверяющего центра – подразделения и/или уполномоченные выделенные работники Банка, ответственные за прием документов на выпуск или отзыв регистрационных свидетельств, идентификацию заявителей и предоставление заявителям доступа к готовым регистрационным свидетельствам.
16. Владелец регистрационного свидетельства (или подписчик Удостоверяющего центра) – физическое или юридическое лицо, действующее в лице своего уполномоченного представителя, как субъект, на имя которого Удостоверяющим центром выдано регистрационное свидетельство, правомерно владеющий закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве.
17. Доверяющие стороны (или пользователи регистрационных свидетельств) – владельцы регистрационных свидетельств или любые другие субъекты, которые действуют, полагаясь на регистрационные свидетельства, выпущенные Удостоверяющим центром, и/или электронные документы с электронными цифровыми подписями, подлинность которых проверяется с помощью этих регистрационных свидетельств.

Раздел 1.4. Назначение регистрационных свидетельств

18. Удостоверяющий центр выпускает регистрационные свидетельства, которые имеют различное назначение, соответствующее разделу 1.1 настоящего Регламента, и, соответственно, разные профили, которые отражаются в расширении “keyUsage” и/или “extendedKeyUsage” регистрационного свидетельства.
19. Кроме этого, для выпускаемых Удостоверяющим центром регистрационных свидетельств, в которых присутствует расширение “cerificatePolicies”, область допустимого применения, в соответствии с разделом 1.4 Политики регистрационных свидетельств, дополнительно ограничивается объектными идентификаторами политики, которые зафиксированы в указанном расширении.
20. Полный перечень объектных идентификаторов политики в клиентских регистрационных свидетельствах приведен на официальном информационном ресурсе Банка в сети Интернет.

Раздел 1.5. Управление документом

21. Настоящий Регламент актуализируется Удостоверяющим центром, расположенным по адресу: A05G1D2, г. Алматы, ул. Панфилова, д. 98, блок Б.

[1] На дату утверждения настоящего Регламента действует приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан «Об утверждении Правил проведения аккредитации удостоверяющих центров» от 1 июня 2020 года № 224/НҚ.
[2] На дату утверждения настоящего Регламента данный функционал выполняет Дирекция криптографической защиты информации Центра обеспечения информационной безопасности Банка.

22. Контактное лицо по вопросам актуализации документа – Руководитель Удостоверяющего центра, A05G1D2, г. Алматы, ул. Панфилова, д. 98, блок Б, +7 (727) 2-598-583 (вн. 12921), alexey.korobetskikh@bcc.kz.
23. Настоящий Регламент применяется в соответствии с Политикой регистрационных свидетельств.
24. Изменения и дополнения в настоящий Регламент готовятся Удостоверяющим центром либо в форме новой редакции, либо в форме перечня изменений и дополнений к текущей редакции Регламента.
25. Перед утверждением изменения и дополнения в настоящий Регламент проходят согласование с заинтересованными подразделениями и должностными лицами Банка согласно внутренним процедурам.
26. Изменения и дополнения в настоящий Регламент утверждаются протокольным решением Правления Банка.
27. Все изменения и дополнения в настоящий Регламент публикуются на официальном информационном ресурсе Банка в сети Интернет.
28. Публикация новой утвержденной редакции Регламента является официальным уведомлением о вступлении ее в силу для пользователей всех регистрационных свидетельств, выпущенных Удостоверяющим центром, включая их владельцев.
29. С даты публикации новой редакции Регламента, если иное не предусмотрено переходными положениями утверждающего решения, изменения и дополнения становятся обязательными для применения пользователями всех регистрационных свидетельств, выпущенных Удостоверяющим центром, включая их владельцев.

Раздел 1.6. Термины, определения и сокращения

30. В настоящем Регламенте используются следующие понятия:
1) аутентификация – процесс или сервис безопасности, реализующий этот процесс, который предназначен для проверки того, что лицо (предмет) является тем, кем себя именует (чем он поименован);
2) Банк – АО «Банк ЦентрКредит»;
3) данные активации – любые данные, за исключением криптографических ключей, которые необходимы для выполнения криптографических операций и требуют защиты: персональные идентификационные номера (PIN), парольные фразы, компоненты разделенного криптографического ключа, биометрические параметры и др.;
4) дерево международных объектных идентификаторов – стандартизированный ITU-T и ISO/IEC механизм (X.660) именования любых реальных или абстрактных объектов однотипными недвусмысленными всеобъемлющими именами, предназначенный для регистрации имен с помощью трех иерархических деревьев особой формы (от 3 разных корней), в которых каждый последующий узел наделен целочисленным номером и ответственен за дальнейшее выделение и регистрацию ветвей, исходящих от него самого;
5) закрытый ключ электронной цифровой подписи – последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи;
6) закрытый криптографический ключ – в криптосистемах с открытым ключом, тот ключ из ключевой пары, который известен только подписчику[3];
7) идентификация – в контексте настоящего Регламента, 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:
• установление соответствия предъявленного лицом имени реально существующей идентичности лица и

[3] Закрытые ключи электронной цифровой подписи являются одной из разновидностей закрытых криптографических ключей.

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

8) 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;

9) компрометация криптографических ключей – утрата владельцем криптографических ключей уверенности в том, что конкретные криптографические ключи обеспечивают безопасность защищаемой с их помощью информации;

10) носитель ключевой информации – в контексте настоящего Регламента, съемный машинный носитель информации (специализированный аппаратный токен, карта памяти, жесткий диск и др.), способный хранить криптографические ключи в электронной форме;

11) объектный идентификатор – идентификатор, который однозначно именует узел дерева международных объектных идентификаторов в форме списка целочисленных значений, упорядоченного от корня дерева к данному узлу;

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

13) открытый криптографический ключ – в криптосистемах с открытым ключом, тот ключ из ключевой пары, который известен публике[4];

14) политика применения регистрационных свидетельств (также именуется Политикой регистрационных свидетельств) – нормативный документ, который представляет собой озаглавленный набор правил, определяющих применимость регистрационного свидетельства в определенной общности (классе) приложений с общими требованиями информационной безопасности;

15) регламент деятельности удостоверяющего центра – нормативный документ, который определяет порядок организации основной деятельности удостоверяющего центра, осуществляемой в соответствии с Политикой регистрационных свидетельств, включая течение основных процессов удостоверяющего центра;

16) регистрационное свидетельство – электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом Республики Казахстан “Об электронном документе и электронной цифровой подписи”;

17) сертификат открытого (криптографического) ключа (далее - сертификат) – открытый криптографический ключ подписчика вместе с дополнительной информацией, идентифицирующей этот ключ и подписчика, подлинность и взаимосвязь которых удостоверена электронной цифровой подписью, сформированной закрытым криптографическим ключом Удостоверяющего центра[5];

---

[4] Открытые ключи электронной цифровой подписи являются одной из разновидностей открытых криптографических ключей.

[5] Понятие “сертификат” введено в соответствии с международным стандартом ITU-T X.509 “Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks” (Информационная технология – Взаимодействие открытых систем – Справочник: структуры сертификатов открытых (криптографических) ключей и атрибутов). Регистрационные свидетельства, выпускаемые Удостоверяющим центром в соответствии с Законом Республики Казахстан “Об электронном документе и электронной цифровой подписи”, являются одной из разновидностей выпускаемых сертификатов. Вместе с тем, в законодательных актах Республики Казахстан не используется терминов, равносильных термину “сертификат открытого (криптографического) ключа”.
В связи с этим, всюду в тексте настоящего Регламента термин “регистрационные свидетельства”, введенный в Законе Республики Казахстан “Об электронном документе и электронной цифровой подписи”, обобщает все возможные разновидности сертификатов открытых (криптографических) ключей, выпускаемых Удостоверяющим центром Банка, т.е. его следует раскрывать как “регистрационные свидетельства и (или) сертификаты открытых (криптографических) ключей иного

18) список отозванных регистрационных свидетельств (CORC) – часть регистра регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва;
19) средства криптографической защиты информации (или СКЗИ) – средства, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами;
20) средства электронной цифровой подписи – совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи[6];
21) токен – в контексте настоящего Регламента, физическое устройство, выдаваемое уполномоченному лицу в целях организации защищенного хранения резервной копии закрытых криптографических ключей и настроек аппаратных криптографических модулей (Hardware Security Module, HSM) Удостоверяющего центра;
22) участники инфраструктуры открытых ключей – совокупность физических и юридических лиц, действующих в лице своих уполномоченных представителей, которые выполняют любую из ролей: пользователя или владельца регистрационного свидетельства (доверяющей стороны или подписчика), центра регистрации или удостоверяющего центра, – в одной и той же инфраструктуре открытых ключей;
23) цепочка регистрационных свидетельств – упорядоченная последовательность регистрационных свидетельств, начинающаяся с регистрационного свидетельства, электронная цифровая подпись в котором может быть проверена с помощью доверенного корневого регистрационного свидетельства, успешная обработка которой с помощью стандартизированного алгоритма позволяет подтвердить принадлежность открытого криптографического ключа лицу, указанному в заключительном регистрационном свидетельстве последовательности, в поле “subject”;
24) электронная цифровая подпись (или ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;
25) электронный документ – документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством ЭЦП.

Глава 2. Ответственность за хранилище и публикацию данных в нем

Раздел 2.1. Хранилище

31. Составной частью информационной системы Удостоверяющего центра является хранилище, которое Удостоверяющий центр использует в качестве справочника информации при предоставлении своих основных сервисов.
32. Кроме этого, Удостоверяющий центр на официальном информационном ресурсе Банка в сети Интернет публикует:
1) Политику регистрационных свидетельств;
2) Настоящий Регламент;
3) Регистрационные свидетельства Удостоверяющего центра;
4) ссылки для доступа к спискам отозванных регистрационных свидетельств.
33. Указанный раздел ресурса используется для размещения иной важной информации Удостоверяющего центра, в целях уведомления владельцев и пользователей регистрационных свидетельств (подписчиков Удостоверяющего центра и доверяющих сторон).

Раздел 2.2. Публикация в хранилище информации о регистрационных свидетельствах

[6] Средства электронной цифровой подписи являются одной из разновидностей средств криптографической защиты информации.

34. В хранилище Удостоверяющего центра в режиме онлайн публикуются все действующие регистрационные свидетельства (валидные регистрационные свидетельства, не имеющие статуса “отозвано”), а также списки отозванных регистрационных свидетельства.

Раздел 2.3. Периодичность актуализации данных в хранилище

35. Каждое регистрационное свидетельство, выпущенное Удостоверяющим центром, публикуется в хранилище автоматически и немедленно (в режиме онлайн).
36. При отзыве регистрационное свидетельство автоматически удаляется из хранилища и переносится в архив.
37. Проверка истечения срока действия всех регистрационных свидетельств, размещенных в хранилище, осуществляется ежесуточно по расписанию, определенному соответствующей настройкой информационной системы Удостоверяющего центра.
38. В случае отзыва любого регистрационного свидетельства Удостоверяющий центр автоматически и немедленно (в режиме онлайн) формирует и публикует в хранилище обновленный список отозванных регистрационных свидетельств.
39. Отозванные регистрационные свидетельства с истекшим сроком действия удаляются из списков отозванных регистрационных свидетельств не реже одного раза в неделю по расписанию, определенному соответствующей настройкой информационной системы Удостоверяющего центра.
40. В условиях отсутствия событий отзыва регистрационных свидетельств новые списки отозванных регистрационных свидетельств формируются и выпускаются еженедельно по расписанию, определенному соответствующей настройкой информационной системы Удостоверяющего центра.

Раздел 2.4. Контроль доступа к хранилищу

41. Доступ для чтения данных из хранилища предоставляется Удостоверяющим центром обслуживаемым информационным системам Банка, по заявкам, в порядке, установленном внутренними нормативными документами Банка по вопросам информационной безопасности, без каких-либо дополнительных ограничений постоянного характера.
42. Доступ для добавления, изменения (удаления) данных в(из) хранилище(-а) предоставляется Удостоверяющим центром для ограниченного круга уполномоченных лиц.
43. В случаях превышения нагрузки на сервис доступа в хранилище соответствующих параметров уровня обслуживания Удостоверяющий центр автоматически применяет временные ограничения доступа в качестве активных мер противодействия кибератакам, иным угрозам перебоя в предоставлении сервисов.
44. Ограничения и контроли доступа в хранилище применяются в соответствии с Политикой информационной безопасности Банка[7].

Глава 3. Идентификация и аутентификация

Раздел 3.1. Требования к именам

45. Используемые Удостоверяющим центром правила именования субъектов обеспечивают идентификацию владельцев регистрационных свидетельств (подписчиков Удостоверяющего центра) во всех выпускаемых регистрационных свидетельствах.
46. Имена субъектов в полях “Issuer” и “Subject” во всех без исключения регистрационных свидетельствах, выпускаемых Удостоверяющим центром, указываются в формате выделенных имен (DN-имен) в соответствии с международными рекомендациями ITU-T X.520.

[7] Политика информационной безопасности опубликована на официальном ресурсе Банка в сети Интернет по адресу https://www.bcc.kz/product/information-security/

47. Атрибуты и содержание полей “Issuer” и “Subject” корневых регистрационных свидетельств Удостоверяющего центра приведены в нижеследующей таблице.

Атрибут	**Значение**
Country (C=)	KZ
Organization (O=)	Bank CenterCredit JSC
Common Name (CN=)	Certification Authority

48. В поле “Issuer” всех некорневых регистрационных свидетельств, выпускаемых Удостоверяющим центром, включаются в точности те же атрибуты и те же значения, что и в поле “Issuer” корневого регистрационного свидетельства.

49. В регистрационные свидетельства подписчиков Удостоверяющего центра в поле “Subject” включается набор атрибутов, который приведен в нижеследующей таблице.

Атрибут	**Значение**
Country (C=)	KZ
Organization (O=)	Bank CenterCredit JSC
Organization unit (OU=)	*Логическая или структурная единица Банка, например, информационная система Банка, ее подсистема, блок, департамент или иное подразделение Банка*
[Common name (CN=)	*Код организации, если владелец регистрационного свидетельства действует от имени юридического лица*]
Unique identification number (UID=)	[*Опциально, идентификатор технического средства в информационной системе, если регистрационное свидетельство выпускается в целях защиты технического средства, и обязательно,*] *код владельца регистрационного свидетельства*

50. Если регистрационное свидетельство выдается юридическому лицу в лице его представителя, то атрибут “Common name” заполняется следующим образом. В буквенно-цифровом формате в нем указывается:

- для резидентов – БИН в формате “BINxxxxxxxxxxxx”, где:

xxxxxxxxxxxx – 12-значный БИН;

- для нерезидентов – реквизиты плательщика НДС в формате “ccxx…xyyyymmddo..o”, где:

cc – двухбуквенный код страны регистрации плательщика НДС согласно ISO 3166-1;
xx..x – регистрационный номер плательщика НДС (VATIN);
yyyymmdd – дата регистрации плательщика НДС в соответствующем формате;
o…o – наименование министерства или ведомства, выдавшего документ о регистрации плательщика НДС, на английском языке в форме общепринятой аббревиатуры.

51. Атрибут “Unique identification number” заполняется следующим образом. Если регистрационное свидетельство выпускается в целях защиты технического средства (сервера, терминала, службы и т.п.), то в качестве префикса указывается уникальный идентификатор, назначенный ему информационной системой Банка. Далее используются данные лица, ответственного за закрытый криптографический ключ, в буквенно-цифровом формате:

- для резидентов – ИИН в формате “IINxxxxxxxxxxxx”, где:

xxxxxxxxxxxx – 12-значный ИИН;

- для нерезидентов – реквизиты паспорта в формате “ccxx…xyyyymmddo..o”, где:

cc – двухбуквенный код страны выдачи паспорта согласно ISO 3166-1;
xx..x – номер паспорта (и его серия, если указана);
yyyymmdd – дата выдачи паспорта, в соответствующем формате;
o…o – наименование министерства или ведомства, выдавшего паспорт, на английском языке в форме общепринятой аббревиатуры.

Если ответственное лицо не имеет ни ИИН, ни паспорта, то используются реквизиты удостоверяющего личность документа, заменяющего паспорт.

Раздел 3.2. Первоначальная проверка идентичности

52. Первоначальная проверка идентичности – это наиболее полная форма процедур идентификации и аутентификации, которая согласно международным отраслевым рекомендациям проводится в отношении подписчика при выпуске первого регистрационного свидетельства.
53. Центры регистрации проводят первоначальную проверку идентичности подписчика в соответствии с правовым актом по вопросам выдачи, хранения, отзыва регистрационных свидетельств, изданным уполномоченным органом в сфере информатизации (далее – Правовой акт регулятора)[8].

Глава 4. Операционные требования к жизненному циклу регистрационных свидетельств

Раздел 4.1. Заявления на выпуск регистрационных свидетельств

54. Принципы оформления заявлений на выпуск регистрационного свидетельства подписчика Удостоверяющего центра определены разделом 4.1 Политики регистрационных свидетельств.
55. Центры регистрации принимают заявления на выпуск регистрационных свидетельств от:
1) уполномоченных представителей юридических лиц;
2) физических лиц, действующих самостоятельно.

Раздел 4.2. Обработка заявлений на выпуск регистрационных свидетельств

56. Центры регистрации обрабатывают заявления на выпуск регистрационного свидетельства в соответствии с Правовым актом регулятора.
57. После регистрации заявление отклоняется, если:
1) заявитель указал в нем не всю информацию, необходимую в соответствии с Правовым актом регулятора;
2) заявитель указал в них недостоверные сведения;
3) центру регистрации или Удостоверяющему центру известно о решении суда, запрещающем выдачу регистрационного свидетельства на имя заявителя;
4) заявитель не достиг возраста шестнадцати лет;
5) в иных случаях, установленных законами Республики Казахстан.
58. В случае изменения определенного законодательством Республики Казахстан перечня оснований для отказа в выдаче регистрационного свидетельства применяются требования законодательства. Настоящий Регламент деятельности Удостоверяющего центра подлежит приведению в соответствие с законодательством в установленном порядке.
59. Заявления на выпуск регистрационных свидетельств рассматриваются центром регистрации и Удостоверяющим центром в общей сложности в срок не более 5 рабочих дней с даты регистрации заявления.

Раздел 4.3. Выпуск регистрационных свидетельств

60. Принципы и основные этапы выпуска регистрационного свидетельства подписчику Удостоверяющего центра определены в разделе 4.3 Политики регистрационных свидетельств.

[8] На дату утверждения настоящего Регламента действует приказ Министра по инвестициям и развитию Республики Казахстан «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» от 23 декабря 2015 года № 1231.

61. Защита ключевой пары заявителя при генерации на стороне центра регистрации достигается за счет ее генерации непосредственно на защищенном носителе ключевой информации, из которого закрытый ключ не может быть извлечен. По окончании процедуры выпуска регистрационного свидетельства защищенный ключевой носитель, содержащий закрытый криптографический ключ и регистрационное свидетельство заявителя, а также регистрационное свидетельство Удостоверяющего центра, работник центра регистрации вручает заявителю лично.
62. Защита открытого ключа владельца регистрационного свидетельства от подмены или искажения в случае необходимости его доставки из центра регистрации в Удостоверяющий центр достигается за счет использования механизма ЭЦП. Открытый ключ включается в контекст запроса на выпуск регистрационного свидетельства, который составляется в формате PKCS#10 и подписывается закрытым ключом.
63. Способом доказательства Удостоверяющему центру факта владения заявителем закрытым криптографическим ключом в случае необходимости служит проверка ЭЦП в электронном запросе формата PKCS#10, которую выполняет Удостоверяющий центр при обработке запроса.

Раздел 4.4. Принятие регистрационных свидетельств

64. Если подписчик в течение 14 календарных дней после выпуска регистрационного свидетельства не обратился в центр регистрации с письменным заявлением (на бумажном носителе) об отзыве этого регистрационного свидетельства или начал использовать соответствующий закрытый ключ до подачи указанного заявления на отзыв, то регистрационное свидетельство автоматически считается принятым подписчиком.

Раздел 4.5. Использование регистрационных свидетельств и ключевых пар

65. Необходимые условия использования регистрационных свидетельств и пар криптографических ключей определены разделом 4.5 Политики регистрационных свидетельств.
66. Перед использованием владелец регистрационного свидетельства (подписчик) выбирает закрытый криптографический ключ в соответствии с содержанием расширений “keyUsage” и “extendedKeyUsage” в соответствующем регистрационном свидетельстве.
67. Для проведения проверки ЭЦП пользователь регистрационного свидетельства (доверяющая сторона) выполняет процедуру, регламентированную Правовым актом регулятора, для чего в частности:
1) определяет и проверяет цепочку регистрационных свидетельств, которая позволяет установить субъекта, сформировавшего ЭЦП. В ходе проверки цепочки регистрационных свидетельств используется алгоритм, изложенный в рекомендациях RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” (Профиль сертификата и списка отозванных сертификатов интернет инфраструктуры открытых ключей формата X.509);
2) в ходе проверки каждого регистрационного свидетельства цепочки дополнительно контролирует содержание расширений “keyUsage” и “extendedKeyUsage” на соответствие цели использования;
3) самостоятельно проверяет наличие у подписавшего лица полномочий, достаточных для подписания электронного документа. Информационная система Удостоверяющего центра сервисов контроля полномочий подписчика не предоставляет.
68. Если любой шаг проверки дает отрицательный результат или его невозможно выполнить, то доверяющая сторона полагает ЭЦП недействительной и отвергает электронный документ.
69. Если в электронном документе имеется отметка времени, сформированная Удостоверяющим центром, то для выполнения действия, требующего доверия к отметке времени, доверяющая сторона также проверяет эту отметку времени в порядке, аналогичном проверке ЭЦП в электронном документе.
70. Если любое из регистрационных свидетельств цепочки на момент проверки ЭЦП имеет статус “отозвано”, только доверяющая сторона исключительно на свой риск решает, оправдано или нет

полагаться на электронный документ, сформированный подписчиком до отзыва одного из регистрационных свидетельств цепочки. Удостоверяющий центр в случаях такого рода не несет ответственности перед пользователями регистрационных свидетельств (доверяющими сторонами), так как подача заявления на отзыв регистрационного свидетельства является обязанностью конкретного владельца регистрационного свидетельства (подписчика).

71. Если обстоятельства указывают на необходимости дополнительных гарантий со стороны авторов электронного документа, то пользователь регистрационного свидетельства (доверяющая сторона) получает такие дополнительные гарантии от владельцев регистрационных свидетельств (подписчиков) самостоятельно, до выполнения действий, требующих доверия к регистрационному свидетельству, и без обращения в Удостоверяющий центр.

Раздел 4.6. Обновление сроков действия в регистрационных свидетельствах

72. Услуг по обновлению сроков действия в регистрационных свидетельствах Удостоверяющий центр не предоставляет.

Раздел 4.7. Смена криптографических ключей в регистрационных свидетельствах

73. Услуг по смене ключей в регистрационных свидетельствах Удостоверяющий центр не предоставляет.

74. Для смены криптографических ключей владелец регистрационного свидетельства (подписчик Удостоверяющего центра) повторно проходит процедуру выпуска (новых) регистрационных свидетельств, в порядке, определенном разделами 4.1, 4.2 и 4.3 настоящего Регламента.

75. Если при этом новое регистрационное свидетельство запрашивается из-за компрометации закрытого криптографического ключа, то сначала владелец регистрационного свидетельства (подписчик Удостоверяющего центра) подает заявление на отзыв скомпрометированного регистрационного свидетельства, а затем заявление на выпуск нового.

Раздел 4.8. Изменение данных в регистрационных свидетельствах

76. Услуг по изменению данных в регистрационных свидетельствах Удостоверяющий центр не предоставляет.

77. Для изменения данных в регистрационном свидетельстве его владелец (подписчик Удостоверяющего центра) повторно проходит процедуру выпуска (новых) регистрационных свидетельств, в порядке, определенном разделами 4.1, 4.2 и 4.3 настоящего Регламента.

78. При этом сначала владелец регистрационного свидетельства (подписчик Удостоверяющего центра) подает заявление на отзыв действующего регистрационного свидетельства, а затем заявление на выпуск нового.

Раздел 4.9. Отзыв регистрационных свидетельств

79. Возможные причины отзыва определяются следующим списком:

1) документальное требование владельца регистрационного свидетельства (подписчика) либо его представителя;
2) установление факта представления недостоверных сведений либо неполного пакета документов при получении регистрационного свидетельства;
3) смерть владельца регистрационного свидетельства (подписчика);
4) изменения фамилии, имени или отчества (если оно указано в документе, удостоверяющем личность) владельца регистрационного свидетельства;
5) смена наименования, реорганизация, ликвидация юридического лица – владельца регистрационного свидетельства, смена руководителя юридического лица;
6) решение суда, вступившее в законную силу[9];

[9] В случаях, перечисленных в подпунктах 3-6 настоящего пункта, основанием для отзыва служит письменное заявление

7) иные причины, предусмотренные Политикой регистрационных свидетельств:

- добровольный отказ подписчика от использования информационных систем Банка и необходимых для этого регистрационных свидетельств;
- наличие у Банка обоснованных подозрений в компрометации закрытых криптографических ключей, соответствующих регистрационному свидетельству;
- наличие доказательств нарушения владельцем регистрационного свидетельства (подписчиком) обязательств, заверений и гарантий Политики регистрационных свидетельств или действующего договора с Банком;
- утрата силы договора, который является необходимым условием владения и пользования подписчиком соответствующим закрытым ключом;
- наличие доказательств выпуска регистрационного свидетельства с существенным нарушением процедур Правового акта регулятора, Политики регистрационных свидетельств, настоящего Регламента, выпуска регистрационного свидетельства неидентифицированному лицу или лицу, идентифицированному ошибочно;
- наличие доказательств ошибочности сведений из заявления на выпуск регистрационного свидетельства;
- утрата актуальности данными заявления на выпуск регистрационного свидетельства;
- продолжение использования регистрационного свидетельства опасно для информационных систем Банка.

80. В случае изменения определенного законодательством Республики Казахстан перечня оснований для отзыва регистрационного свидетельства применяются требования законодательства. Настоящий Регламент подлежит приведению в соответствие с законодательством в установленном порядке.

81. Центры регистрации и Удостоверяющий центр обрабатывают заявления на отзыв регистрационного свидетельства, оформленные от лица:

1) владельца регистрационного свидетельства;
2) физических лиц, являющихся уполномоченными представителями владельца регистрационного свидетельства;
3) работника центра регистрации.

82. Перед отзывом регистрационного свидетельства центр регистрации и/или Удостоверяющий центр проверяет полномочия инициатора запрашивать отзыв, включая идентификацию заявителя. При этом применяется механизм идентификации, указанный в разделе 3.2 настоящего Регламента.

83. Процедура отзыва регистрационного свидетельства осуществляется в соответствии с Правовым актом регулятора. В случае обоснованности заявления, регистрационное свидетельство отзывается не позднее рабочего дня, следующего за датой поступления заявления на отзыв регистрационного свидетельства.

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

85. Для обеспечения непрерывной возможности проверки статуса регистрационных свидетельств доверяющими сторонами Удостоверяющий центр:

1) публикует обновляемые списки отозванных регистрационных свидетельств;
2) обеспечивает функционирование службы протокола OCSP[10].

86. Услуг по временному приостановлению или возобновлению действия регистрационных свидетельств Удостоверяющий центр не предоставляет.

на отзыв регистрационного свидетельства (на бумажном носителе) с предъявлением оригинала официального документа уполномоченной инстанции, подтверждающего наличие оснований (например, свидетельство о смерти, справка о перерегистрации юридического лица, решение суда и др.). Удостоверяющий центр и центры регистрации не проводят мониторинг информационных ресурсов, содержащих сведения соответствующего рода.

[10] OCSP – сервис для получения информации о статусе регистрационных свидетельств, выпущенных Удостоверяющим центром (согласно рекомендациям RFC 2560 “X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP”, онлайн протокол статуса сертификатов интернет инфраструктуры открытых ключей X.509).

87. Услуг по депонированию закрытого ключа владельца регистрационного свидетельства (подписчика) Удостоверяющий центр не предоставляет.

Глава 5. Физический, операционный и управляющие контроли

Раздел 5.1. Физический контроль

88. Детальные меры физического контроля Удостоверяющего центра определены и утверждены внутренними документами Банка и в настоящем Регламенте не раскрываются. В данной главе приведен общий обзор этих мер.
89. Информационная система удостоверяющего центра обеспечена двумя центрами обработки данных (основной и резервный), расположенными на разных объектах в целях резервирования и восстановления функционирования в случае чрезвычайной ситуации.
90. Физический доступ в основной и резервный центры обработки данных организованы и контролируются одинаковыми мерами безопасности.
91. 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.

Раздел 5.2. Операционный контроль

92. Центры обработки данных Удостоверяющего центра обеспечиваются круглосуточной технической поддержкой в режиме 24/7/365, включающей перезагрузку оборудования и замену комплектующих.
93. По соглашению об уровне обслуживания допустимое время простоя оборудования в центрах обработки данных по причине отказов оборудования и каналов связи составляет не более 18 часов в год (99.8%) за исключением плановых работ по модернизации или форс-мажорных обстоятельств, неподконтрольных поставщикам услуг.
94. Время реакции поставщика услуг центров обработки данных – не более 1 часа с момента оформления заявки Удостоверяющим центром.
95. Из всего набора рабочих процедур Удостоверяющего центра особыми организационными мерами выделены процедуры настройки и обслуживания аппаратных криптографических модулей (Hardware Security Module, HSM) и их ключевого материала.
96. С момента ввода в устройства HSM криптографических ключей для физического доступа к HSM и ключам требуется участие минимум двоих уполномоченных работников Банка.
97. Работники, осуществляющие операционный контроль работы HSM, не работают с криптографическими ключами физически и наоборот.

Раздел 5.3. Контроль персонала

98. Перед назначением на должности в Удостоверяющем центре и центрах регистрации соискатели предоставляют документы, определенные Трудовым кодексом Республики Казахстан и проходят скрининг в соответствии с внутренним документом Банка по подбору персонала[11].

[11] На дату утверждения настоящего Регламента действует Положение по подбору, приему и адаптации персонала АО «Банк ЦентрКредит», утвержденная Решением Правления от 09.07.2020 г. №3-0709-04.

99. Специалисты и руководители Удостоверяющего центра проходят обучение или сертификацию не реже одного раза в три года.
100. Ответственность работников Удостоверяющего центра за несанкционированный доступ к служебной информации и иные нарушения требований информационной безопасности предусмотрена трудовым договором и должностными инструкциями
101. Дисциплинарные взыскания по факту нарушения требований информационной безопасности определяются и выносятся приказами в соответствии с внутренним документом Банка[12].
102. Каждому работнику Удостоверяющего центра и центров регистрации для компетентного исполнения должностных обязанностей обеспечивается доступ к текстам правовых актов законодательства и внутренних документов Банка.

Раздел 5.4. Процедуры контрольного протоколирования

103. Типы событий, подлежащих протоколированию, определены разделом 5.4 Политики регистрационных свидетельств.
104. Структура записи контрольного протокола включает в себя:
1) дату и время записи;
2) порядковый номер записи;
3) идентичность сущности, которая инициировала событие, подлежащее протоколированию;
4) тип события;
5) источник записи.
105. Контрольные протоколы информационной системы Удостоверяющего центра ведутся непрерывно, подлежат ежесуточному резервному копированию, ежемесячному архивированию и сдаче в архив в соответствии с разделом 5.5 настоящего Регламента, где хранятся в течение регламентированного срока.
106. Перед записью на машинный носитель архивная копия контрольных протоколов информационной системы Удостоверяющего центра зашифровывается и снабжается кодом аутентификации.
107. Документальные материалы владельцев регистрационных свидетельств (подписчиков) и контрагентов Удостоверяющего центра регистрируются, систематизируются и хранятся в соответствии с внутренним документом Банка по вопросам делопроизводства[13].

Раздел 5.5. Ведение архива

108. Удостоверяющий центр ведет архив, в котором хранит письменные и электронные документы, определенные разделом 5.5 Политики регистрационных свидетельств.
109. Хранение носителей архивной информации, маркировка архивных носителей информации, защита данных архива от несанкционированного просмотра, изменения и удаления осуществляются в соответствии с внутренним документом Банка по вопросам резервирования данных информационных систем[14].
110. Утилизация носителей конфиденциальных данных Удостоверяющего центра осуществляется в соответствии с внутренним документом Банка по вопросам уничтожения данных[15].

---

[12] На дату утверждения настоящего Регламента действует Процедура о дисциплинарной ответственности работников АО «Банк ЦентрКредит», утвержденная Решением Правления от 04.02.2021 № 3-0204-01.
[13] На дату утверждения настоящего Регламента действуют Правила документирования, управления документацией и использования систем электронного документооборота в АО «Банк ЦентрКредит», утвержденные Решением Правления от 23.04.2019 №3-0423-01.
[14] На дату утверждения настоящего Регламента действует Процедура резервного копирования и восстановления информации файловых ресурсов и баз данных АО «Банк ЦентрКредит», утвержденная Решением Правления от 06.08.2018 №599.
[15] На дату утверждения настоящего Регламента действует Процедура уничтожения информации в электронной (цифровой) форме на технических носителях в АО «Банк ЦентрКредит», утвержденная Решением Правления от 13.12.2021 №3-1213-02.

Раздел 5.6. Смена криптографических ключей удостоверяющего центра

111. Смена криптографических ключей осуществляется в соответствии с эксплуатационно-технической документацией аппаратных криптографических модулей (HSM) Удостоверяющего центра.

Раздел 5.7 Восстановление функционирования в случае чрезвычайных происшествий или компрометации

112. В случае чрезвычайных происшествий, влекущих прерывание функционирования сервисов Удостоверяющего центра, принимается решение о вводе в действие Плана восстановления функционирования Удостоверяющего центра.
113. В Плане восстановления функционирования Удостоверяющего центра предусмотрены:
1) выбор площадки для восстановления на базе основного или резервного центров обработки данных;
2) восстановление рабочих записей из резервной или архивной копии.
114. Резервный центр обработки данных обеспечен запасным оборудованием. Создание и хранение резервных и архивных копии рабочих записей Удостоверяющего центра, а также форма Плана восстановления функционирования регламентированы внутренним документом Банка по вопросам резервирования данных информационных систем[16].
115. 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.
116. В случае принятия Удостоверяющим центром решения об отзыве регистрационного свидетельства криптографических ключей Удостоверяющего центра выполняются следующие процедуры:
1) информация об отзыве публикуется в списке отозванных регистрационных свидетельств в соответствии с разделом 4.9 настоящего Регламента;
2) в соответствии с Планом восстановления функционирования предпринимаются иные целесообразные меры для дополнительного уведомления доверяющих сторон об отзыве регистрационного свидетельства УЦ;
3) за исключением случаев прекращения деятельности Удостоверяющего центра генерируются новые криптографические ключи в соответствии с разделом 6.1 настоящего Регламента.
117. Актуальность Плана восстановления функционирования Удостоверяющего центра проверяется по мере внесения изменений в информационную систему Удостоверяющего центра или по результатам переключения информационной системы Удостоверяющего центра между основным и резервным центрами обработки данных, но не реже одного раза в год.

Раздел 5.8. Прекращение работы удостоверяющего центра

118. В случае принятия решения о прекращение работы Удостоверяющего центра уведомление владельцев регистрационных свидетельств (подписчиков Удостоверяющего центра), передача и архивное хранение записей Удостоверяющего центра организовываются в соответствии со ст. 22 Закона Республики Казахстан «Об электронном документе и электронной цифровой подписи».

Глава 6. Технический контроль безопасности

Раздел 6.1. Генерация и установка криптографических ключей

[16] На дату утверждения настоящего Регламента действует Процедура резервного копирования и восстановления информации файловых ресурсов и баз данных АО «Банк ЦентрКредит», утвержденная Решением Правления от 06.08.2018 №599.

119. По каждому факту генерации криптографических ключей Удостоверяющего центра составляется протокол, который датируется и подписывается лицами, принимавшими участие в процедуре. Протоколы хранятся в соответствии с внутренним документом Банка по вопросам делопроизводства.
120. Доступ работников или информационной системы Удостоверяющего центра к закрытым криптографическим ключам владельцев регистрационных свидетельств (подписчиков Удостоверяющего центра) технически исключен использованием только защищенных носителей ключевой информации.
121. Целостность и принадлежность открытых криптографических ключей Удостоверяющего центра и его подписчиков на этапе от их генерации до выпуска регистрационных свидетельств защищаются механизмом электронной цифровой подписи. Открытые ключи передаются от подписчиков в Удостоверяющий центр только в форме электронных документов формата PKCS#10.
122. Открытые криптографические ключи Удостоверяющего центра передаются доверяющим сторонам в форме регистрационных свидетельств.
123. Владельцы регистрационных свидетельств (подписчики Удостоверяющего центра) могут запросить открытые криптографические ключи Удостоверяющего центра из рук в руки в центре регистрации, отдельно или как часть цепочки к собственному регистрационному свидетельству.
124. Открытые криптографические ключи Удостоверяющего центра (в составе регистрационных свидетельств) также доступны для загрузки с официального информационного ресурса Банка в сети Интернет.
125. Удостоверяющий центр регистрирует криптографические ключи, предназначенные для использования в соответствии с:
1) международным стандартом ГОСТ 34.310-2004 (ЭЦП).
Длина закрытого ключа – 256 двоичных разрядов.
Длина открытого ключа – 512 двоичных разрядов;
2) международными рекомендациями PKCS#1 (RFC 8017).
Длина закрытого ключа – не менее 2048 двоичных разрядов.
Длина открытого ключа – не менее 2048 двоичных разрядов.

Раздел 6.2. Защита закрытых криптографических ключей и инженерные контроли криптографических модулей

126. Генерация закрытых криптографических ключей Удостоверяющего центра производится непосредственно в том аппаратном криптографическом модуле (HSM), в котором эти ключи будут впервые использованы. Дополнительной активации вновь сгенерированных закрытых ключей не требуется.
127. Согласно требованию Политики регистрационных свидетельств, закрытые криптографические ключи Удостоверяющего центра после создания не подлежат депонированию. Вместе с тем, в целях обеспечения возможности восстановления функционирования информационной систем после чрезвычайного происшествия или иного сбоя в работе Удостоверяющий центр непосредственно после генерации каждого нового закрытого криптографического ключа создает и хранит резервную копию всех используемых в текущий момент закрытых криптографических ключей.
128. В ходе создания резервной копии закрытые криптографические ключи зашифровываются и выгружаются из аппаратного криптографического модуля (HSM) в зашифрованном виде, в ходе восстановления – в обратном порядке, резервная копия загружается в HSM в зашифрованном виде, и закрытые ключи расшифровываются внутри устройства.
129. При выгрузке резервной копии закрытых ключей Удостоверяющего центра из аппаратного криптографического модуля (HSM) создается секрет (данные активации), который делится на n частей. Для активации ключей после их восстановления из резервной копии достаточно

задействования m частей секрета при участии их хранителей. Текущее значение параметров m и n зафиксировано в паспорте HSM[17].

130. Должностной состав хранителей частей секрета и резервных копий закрытых ключей Удостоверяющего центра фиксируется в протоколе генерации криптографических ключей Удостоверяющего центра.

131. В целях обеспечения непрерывности функционирования информационной системы Удостоверяющего центра закрытые криптографические ключи в аппаратных криптографических модулях (HSM) после их генерации или восстановления из резервной копии остаются активированными до момента уничтожения (удаления).

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

133. Резервные копии закрытых криптографических ключей Удостоверяющего центра, утратившие актуальность вследствие замены или истечения срока действия, не подлежат архивному хранению и уничтожаются в соответствии с внутренним документом Банка по вопросам уничтожения данных[18].

134. Аппаратные криптографические модули (HSM), в которых когда-либо находились закрытые криптографические ключи продуктивной среды Удостоверяющего центра, выведенные из эксплуатации вследствие истечения срока эксплуатации или не поддающиеся ремонту после поломки, за исключением тестовых HSM, не подлежат выбытию из Банка или повторному использованию в любом ином качестве, включая разукомплектование на отдельные узлы и детали. После списания с баланса вышеуказанные HSM подлежат уничтожению в соответствии с внутренним документом Банка по вопросам уничтожения данных.

Раздел 6.3. Прочие аспекты управления криптографическими ключами

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

136. Владельцы и пользователи регистрационных свидетельств (подписчики Удостоверяющего центра и доверяющие стороны) не используют регистрационное свидетельство (криптографические ключи) после истечения срока его действия (срока действия соответствующего им регистрационного свидетельства), за исключением целей, перечисленных в предыдущем пункте.

137. Остальные аспекты управления криптографическими ключами определены разделом 6.3 Политики регистрационных свидетельств.

Раздел 6.4. Данные активации

138. Для использования закрытого криптографического ключа подписчику Удостоверяющего центра необходимо создать и применять данные активации в форме пароля.

139. Пароли для активации закрытого криптографического ключа владельца регистрационного свидетельства (подписчика Удостоверяющего центра) используются в соответствии с требованиями внутреннего документа Банка[19].

---

[17] На момент издания настоящего Регламента n = 3 и m = 2.

[18] На дату утверждения настоящего Регламента действует Процедура уничтожения информации в электронной (цифровой) форме на технических носителях в АО «Банк ЦентрКредит», утвержденная Решением Правления от 13.12.2021 №3-1213-02.

[19] На дату утверждения настоящего Регламента действует Процедура управления учетными записями и паролями в АО «Банк ЦентрКредит», утвержденная Решением Правления от 19.07.2021 №3-0719-03.

140. Каждый хранитель части секрета, которая предназначена для активации закрытых криптографических ключей Удостоверяющего центра, хранит свой пароль в тайне и несет ответственность за нарушение данного требования, предусмотренную трудовым договором и должностной инструкцией.
141. Аппаратные токены, содержащие данные активации закрытых криптографических ключей Удостоверяющего центра, в случае утраты актуальности данных активации перезаписываются (обнуляются) и хранятся в порядке, предусмотренном для хранения резервных копий паролей, до момента повторного использования в тех же целях или до списания с обязательным последующим уничтожением. Выбытию из Банка, разукомплектованию или повторному использованию в иных целях защищенные носители, когда-либо использовавшиеся для хранения частей секрета, не подлежат.

Раздел 6.5. Контроль безопасности вычислительных ресурсов

142. Вычислительные ресурсы, программное обеспечение и данные информационной системы Удостоверяющего центра защищаются от несанкционированного доступа в соответствии с Политикой информационной безопасности Банка и в настоящем Регламенте не раскрываются. Общий обзор этих мер приведен в разделе 6.5 Политики регистрационных свидетельств.

Раздел 6.6. Контроль управления развитием и безопасностью

143. Все прикладное программное обеспечение, которое использует в своей деятельности Удостоверяющий центр, является лицензионным, исключительные права на него Банку не принадлежат.
144. Обязательства по обеспечению надлежащего функционирования указанного программного обеспечения выполняет поставщик по договору (сервисная организация).

Раздел 6.7. Контроль безопасности сети

145. Функции Удостоверяющего центра выполняются в корпоративной сети Банка, защищенной от несанкционированного доступа и вмешательства в соответствии с внутренним документом Банка.
146. Схема взаимодействия модулей (компонент) удостоверяющего центра с пояснительной запиской приведена в приложении 1 к настоящему Регламенту.

Раздел 6.8. Метки времени

147. Информация о дате и времени, содержащаяся в регистрационных свидетельствах, списках отозванных регистрационных свидетельств, квитанциях (ответах службы) OCSP, заверяется ЭЦП.

Глава 7. Профили регистрационных свидетельств, CORC и OCSP

Раздел 7.1. Профили регистрационных свидетельств

148. Регистрационные свидетельства, выпускаемые Удостоверяющим центром, соответствуют рекомендациям RFC 3280 с маркировкой по версии 3 (v.3).
149. Основные поля, содержащиеся в регистрационных свидетельствах, вместе с требованиями к их содержанию приведены в нижеследующей таблице.

Название	Требования к содержанию
Version	V3
serialNumber	*уникальный серийный номер регистрационного свидетельства*

signatureAlgorithm	*объектный идентификатор криптографического алгоритма, для которого предназначен ключ, указанный в поле subjectPublicKeyInfo*
Issuer	C=KZ O=Bank CenterCredit JSC CN=Certification Authority
Validity	*YYYYMMDDHHMMSSZ GMT (действителен с)* *YYYYMMDDHHMMSSZ GMT (действителен по)*
Subject	C=KZ O=Bank CenterCredit JSC OU=*Логическая или структурная единица Банка, например, информационная система или подсистема Банка, блок, департамент или иное подразделение Банка* [CN=*Код организации, если подписчик действует от имени юридического лица*] UID=[*Опциально, идентификатор технического средства в информационной системе, если регистрационное свидетельство выпускается в целях защиты технического средства, и далее, обязательно,*] *код подписчика*
subjectPublicKeyInfo	*открытый ключ*
issuerSignatureAlgorithm	*объектный идентификатор криптографического алгоритма, которым подписано регистрационное свидетельство*
signatureValue	*электронная цифровая подпись*

150. Наличие опциального атрибута CN в выделенном имени поля “subject” означает, что физическое лицо (или техническое средство), указанное в обязательном атрибуте UID (уникальный идентификатор), имеет полномочия и действует от имени юридического лица (принадлежит юридическому лицу).

151. Если регистрационное свидетельство выпускается в целях защиты технического средства (сервера, терминала, службы и т.п.), то в атрибуте “Unique identification number” в качестве префикса указывается уникальный идентификатор, назначенный ему информационной системой Банка.

152. Имена, которые указываются в регистрационных свидетельствах, выпускаемых Удостоверяющим центром, соответствуют требованиям раздела 3.1 в соответствии с форматом имен ITU-T X.520.

153. Основные расширения, используемые в регистрационных свидетельствах, вместе с требованиями к их синтаксису приведены в нижеследующей таблице.

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

154. Криптографические алгоритмы, применяемые Удостоверяющим центром для подписи регистрационных свидетельств, приведены в нижеследующей таблице.

Название	Формат
ГОСТ 34.310-2004	{iso(1) member-body(2) kz(398) certification-authorities(3) basic-cryptography(10) algorithms(1) digital-signature(1) GOST-34.310-2004(1)}
SHA-256 with RSA Encryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs-1(1) Sha256WithRSAEncryption(11)}

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

156. Объектные идентификаторы Политики регистрационных свидетельств, соответствующие информационным системам, в которых применяются регистрационные свидетельства, выпущенные Удостоверяющим центром, устанавливаются в соответствии с разделом 1.4 настоящего Регламента. Расширение регистрационных свидетельств “certificatePolicies” заполняется в соответствии с указанным разделом.

Раздел 7.2. Профили списка отозванных регистрационных свидетельств

157. Списки отозванных регистрационных свидетельств, выпускаемые Удостоверяющим центром, соответствуют рекомендациям RFC 3280 с маркировкой по версии 2 (v.2).

158. Основные поля и расширения, содержащиеся в списках отозванных регистрационных свидетельств, вместе с требованиями к их содержанию приведены в нижеследующей таблице.

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

159. Расширения, используемые в записях списка отозванных регистрационных свидетельств, которые выпускает Удостоверяющий центр, приведены в нижеследующей таблице.

Название	Критичность
reasonCode	FALSE
certificateIssuer	FALSE

Раздел 7.3. Профиль сервиса OCSP

160. Сервис OCSP для получения информации о статусе регистрационных свидетельств, выпущенных Удостоверяющим центром, предоставляется в формате версии 1 (согласно

рекомендациям RFC 2560 “X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP”, Онлайн протокол статуса сертификатов интернет инфраструктуры открытых ключей X.509).

Глава 8. Проверка деятельности

161. Аккредитация удостоверяющего центра осуществляется сроком на три года[20] в соответствии с правовым актом уполномоченного органа[21].
162. Кроме этого, деятельность Центра обеспечения информационной безопасности, в состав которого входит Удостоверяющий центр, на плановой основе подвергается внутреннему аудиту в соответствии с внутренним документом Банка.

Глава 9. Прочие вопросы

Раздел 9.1. Тарифы

163. Удостоверяющий центр предоставляет пользователям обслуживаемых информационных систем следующие услуги:
1) выпуск регистрационных свидетельств подписчиков по заявлениям юридических и физических лиц, включая регистрацию заявлений;
2) отзыв регистрационных свидетельств;
3) размещение регистрационных свидетельств и списков отозванных регистрационных свидетельств в хранилище, а также публикация на информационном ресурсе Банка в сети Интернет Политики регистрационных свидетельств, настоящего Регламента и иной актуальной клиент-ориентированной информации об услугах;
4) предоставление информации о статусе регистрационных свидетельств в режиме онлайн по протоколу OCSP;
5) привязка данных к реальному времени в режиме онлайн по протоколу TSP (Time stamp protocol - сервис “метки времени”).
164. Услуги удостоверяющего центра не тарифицируются и не оплачиваются.

Раздел 9.2. Ответственность

165. Ответственность участников инфраструктуры открытых ключей, обслуживаемой Удостоверяющим центром, установлена законодательством Республики Казахстан[22].
166. Ответственность персонала Удостоверяющего центра и центров регистрации установлена трудовым договором и должностными инструкциями.

Раздел 9.3. Конфиденциальность

167. За исключением информации, доступной в хранилище Удостоверяющего центра, иная информация о деятельности Удостоверяющего центра классифицируется в качестве конфиденциальной в соответствии с внутренним документом Банка по вопросам отнесения тех или иных сведений к банковской/коммерческой тайне[23]. Этим же документом регламентируется ответственность и порядок обращения с указанной информацией.
168. Форма заявления на выпуск регистрационного свидетельства подтверждает согласие заявителя на сбор и обработку его персональных данных в соответствии с законодательством

[20] Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи», статья 20-2.
[21] На дату утверждения настоящего Регламента действуют «Правила проведения аккредитации удостоверяющих центров», утвержденные приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 01 июня 2020 года № 224/НҚ.
[22] Кодекс Республики Казахстан «Об административных правонарушениях», статья 640.
[23] На дату утверждения настоящего Регламента действуют Перечень сведений, составляющих банковскую/коммерческую тайну, утвержденные постановлением Совета Директоров от 15.06.2018 года № 153.

Республики Казахстан по вопросам персональных данных и их защиты[24], в том числе дает Удостоверяющему центру разрешение на публикацию регистрационных свидетельств заявителя и информации об их статусе в хранилище.

Раздел 9.4. Защита персональных данных участников

169. Удостоверяющий центр обеспечивает защиту персональных данных участников инфраструктуры открытых ключей в соответствии с законодательством Республики Казахстан по вопросам персональных данных и их защиты.

Раздел 9.5. Права интеллектуальной собственности

170. Удостоверяющий центр не запрещает владельцам и пользователям регистрационных свидетельств (подписчикам Удостоверяющего центра и доверяющим сторонам) копирование и распространение регистрационных свидетельств на неисключительной бесплатной основе, при соблюдении условий полноты и целостности данных.
171. Закрытый криптографический ключ, который соответствует регистрационному свидетельству, выпущенному Удостоверяющим центром, является собственностью владельца этого регистрационного свидетельства (подписчика). Соответствующий ему открытый криптографический ключ и регистрационное свидетельство являются собственностью Банка.

Раздел 9.6. Гарантии и заверения

172. 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) требованиям: действующего законодательства Республики Казахстан по вопросам электронного документа и электронной цифровой подписи, Политики регистрационных свидетельств и настоящего Регламента;
3) публикацию требований Политики регистрационных свидетельств и настоящего Регламента на официальном информационном ресурсе Банка в сети Интернет.
173. Центр регистрации обеспечивает:
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 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 подписчиков на выпуск и отзыв регистрационных свидетельств, процедуры идентификации заявителей, выдача регистрационных свидетельств подписчику) требованиям: действующего законодательства Республики Казахстан по вопросам электронного документа и электронной цифровой подписи, Политики регистрационных свидетельств и настоящего Регламента.
174. Удостоверяющий центр и центры регистрации в своей деятельности выполняют условия гарантий и заверений владельца и пользователя регистрационных свидетельств (подписчика и доверяющей стороны), изложенные в разделе 9.6 Политики регистрационных свидетельств.

Раздел 9.7. Отказ от гарантий

[24] Закон Республики Казахстан «О персональных данных и их защите», статья 8.

175. Удостоверяющий центр не несет перед владельцами и пользователями регистрационных свидетельств (подписчиками 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 и задекларирована Политикой регистрационных свидетельств.

Раздел 9.8 Ограничение ответственности

176. Участники инфраструктуры открытых ключей не несут ответственности за непрямой, особый, случайный или вытекающий ущерб и упущенную выгоду.

Раздел 9.9. Компенсации

177. В части, не противоречащей действующему законодательству Республики Казахстан, на счет центров регистрации относятся расходы, связанные с компенсацией за:
1) подтверждение ошибочной, вводящей в заблуждение или заведомо ложной информации в заявлениях на выпуск или отзыв регистрационного свидетельства;
2) непреднамеренное или умышленное сокрытие существенных фактов, подлежащих отражению в заявлении на выпуск или отзыв регистрационного свидетельства.

Раздел 9.10. Вступление в силу и прекращение действия

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

Раздел 9.11. Уведомления и связь с участниками

181. Участники инфраструктуры открытых ключей: Удостоверяющий центр, центры регистрации, владельцы и пользователи регистрационных свидетельств (подписчики и доверяющие стороны), - для связи друг с другом используют любые целесообразные каналы, соответствующие предмету взаимодействия, степени важности и срочности коммуникации, если иное не определено соглашением между сторонами.

Раздел 9.12. Изменения и дополнения

182. Незначительные изменения в настоящий Регламент (изменение адресов и ссылок, контактной информации, исправление опечаток и т.п.) вносятся без предварительного уведомления участников инфраструктуры открытых ключей. Решения об уровне значимости изменений и дополнений (существенные или несущественные) принимаются Удостоверяющим центром самостоятельно.
183. Существенные изменения и дополнения в настоящий 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 изменения в законодательстве Республики Казахстан.

Раздел 9.13. Разрешение споров

184. Споры между участниками инфраструктуры открытых ключей: между владельцами и пользователями регистрационных свидетельств (подписчиками и доверяющими сторонами), а также между подписчиком или доверяющей стороной, с одной стороны, и Удостоверяющим центром или центром регистрации, с другой стороны, - разрешаются в соответствии с положениями законодательства Республики Казахстан.
185. Если спор не решен в досудебном порядке, то он подлежит разрешению в судебном порядке.

Раздел 9.14. Юрисдикция

186. Для разрешения споров, предметом которых являются разногласия по существу настоящего Регламента, применяется законодательство Республики Казахстан.

Раздел 9.15. Соответствие применимому законодательству

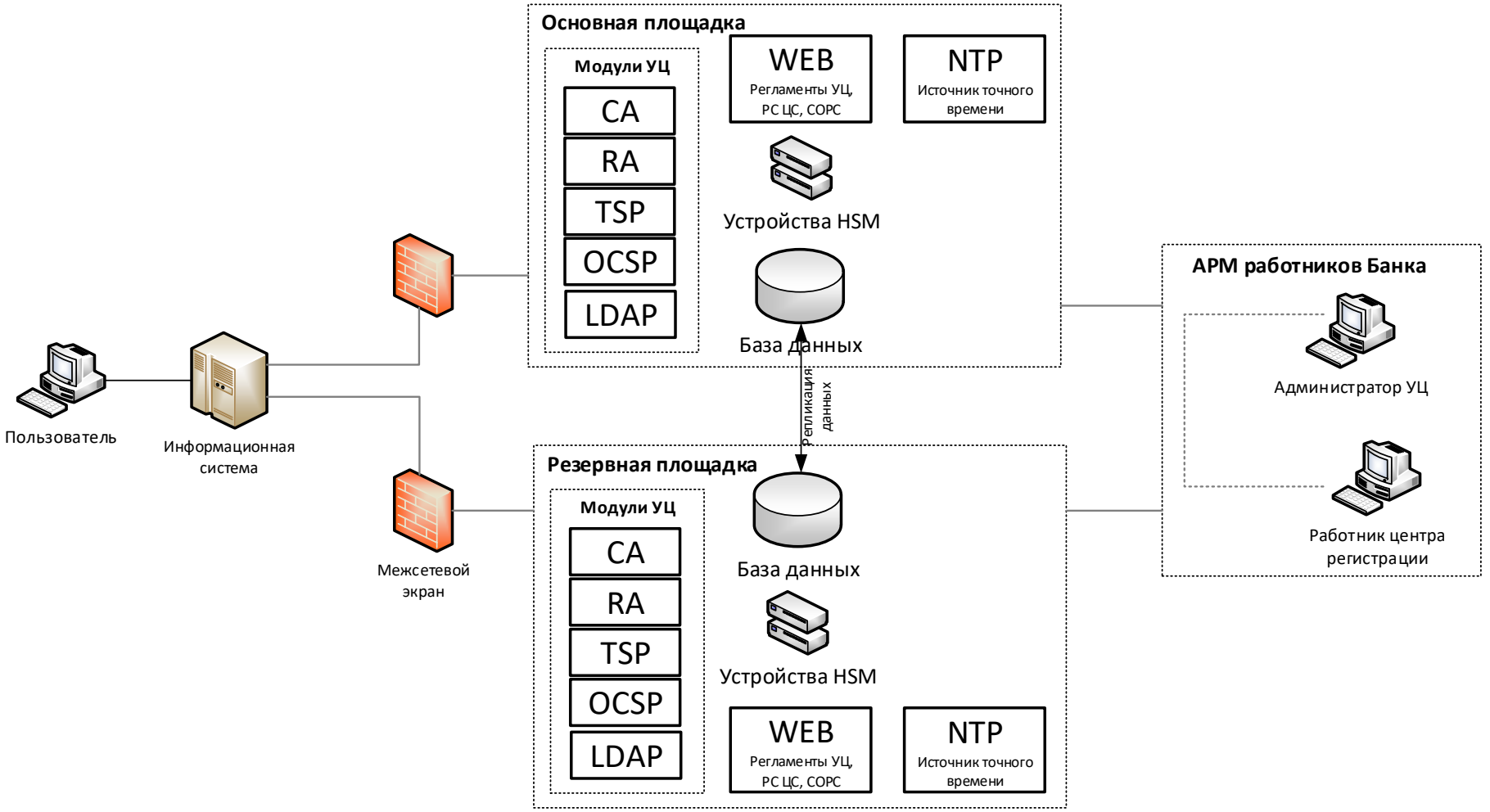
187. К участникам инфраструктуры открытых ключей: Удостоверяющему центру, центрам регистрации, владельцам и пользователям регистрационных свидетельств (подписчикам и доверяющим сторонам), - применимы требования законодательства Республики Казахстан по вопросам:
1) электронного документа и электронной цифровой подписи;
2) разрешений и уведомлений (в части, касающейся реализации СКЗИ);
3) платежей и платежных систем;
4) персональных данных и их защиты.

Раздел 9.16. Прочие положения

188. В случае если часть положений настоящего Регламента будет признана неприменимой судом или уполномоченным государственным органом, остальная их часть сохраняет силу.
189. В случае наступления обстоятельств непреодолимой силы (форс-мажор) участники инфраструктуры открытых ключей: Удостоверяющий центр, центры регистрации, владельцы и пользователи регистрационных свидетельств (подписчики и доверяющие стороны), - руководствуются соответствующими положениями действующих между ними договоров (при наличии).

Приложение 1
к Регламенту деятельности удостоверяющего центра АО «Банк ЦентрКредит»

Схема взаимодействия модулей (компонент) удостоверяющего центра



ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к Схеме взаимодействия модулей (компонент) удостоверяющего центра

Взаимодействие компонентов (основной и резервный центр)

Взаимодействие модулей информационной системы удостоверяющего центра (далее – УЦ) с хранилищем УЦ для публикации и поиска регистрационных свидетельств, списков отозванных регистрационных свидетельств осуществляется по протоколу LDAP.

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

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

Для хранения и обеспечения безопасности закрытых ключей УЦ используются защищенные программно-аппаратные комплексы HSM, соответствующие 2 уровню безопасности согласно СТ РК 1073-2007.

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

Взаимодействие между рабочим и резервным серверами центров обработки данных

Хранение и управление данными обеспечивается СУБД MySQL. Между основным и резервным центрами средствами СУБД в режиме реального времени выполняется репликация данных, что повышает отказоустойчивость системы. Защита реплицируемых данных обеспечивается шифрованием с применением протокола TLS.

Взаимодействие пользователей с УЦ

Пользователи УЦ напрямую с сервисами УЦ не взаимодействуют.

Взаимодействие осуществляется через целевые (обслуживаемые) информационные системы Банка, которые имеют возможность взаимодействия с LDAP-хранилищем и модулями УЦ с использованием протоколов LDAP и HTTP(S).

Взаимодействие сотрудников УЦ с модулями УЦ

Взаимодействие сотрудников УЦ с модулями УЦ осуществляется посредством специализированного программного обеспечения с использованием протоколов LDAP и HTTP(S).

Доступ с рабочего места сотрудника к модулям УЦ возможен только при наличии действующего регистрационного свидетельства с определенными свойствами.

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

Приложение 2
к Регламенту деятельности удостоверяющего центра АО «Банк ЦентрКредит»

Схемы электронной цифровой подписи с данными о применяемых алгоритмах криптографических преобразований и другими исходными данными (основными требованиями) по реализации процесса формирования электронной цифровой подписи и требованиями к отдельным параметрам и удостоверяющему центру