

УТВЕРЖДАЮ
Председатель Правления
АО ЮниКредит Банка
_____ А.А. Оборин
« » _____ 2026 г.

Регламент Удостоверяющего центра
АО ЮниКредит Банка, подчиненного подсистеме
Удостоверяющего центра платформы Цифрового рубля
Банка России

Редакция 1 (0.1, 21.05.2026)

Москва, 2026

Содержание

1. Термины, определения и сокращения.....	3
2. Общие положения.....	8
3. Присоединение к Регламенту.....	8
4. Публикация Регламента	9
5. Порядок внесения изменений в Регламент.....	9
6. Прекращение деятельности ПУЦ.....	10
7. Основные функции ПУЦ.....	10
8. Условия конфиденциальности.....	11
9. Права и обязанности ПУЦ	12
10. Права и обязанности СИО	14
11. Ответственность сторон	15
12. Сроки действия криптографических ключей и СКП ЭП.....	16
13. Хранение СКП ЭП в ПУЦ.....	17
14. Регистрация СИО в Реестре ПУЦ	17
15. Порядок создания и выдачи СКП ЭП СИО.....	17
16. Отзыв СКП ЭП СИО.....	20
17. Смена криптографических ключей ПУЦ	21
18. Смена криптографических ключей СИО.....	21
19. Порядок действий владельца СКП ЭП при компрометации его ключа ЭП	22
20. Содержание и форма СКП ЭП.....	22
21. Хранение материалов	23
Приложение 1.	24
Приложение 2.	28
Приложение 3.	30
Приложение 4.	32

1. Термины, определения и сокращения

1.1. Термины и определения

Аутентификация – процедура установления подлинности источника информации.

Владелец сертификата ключа проверки электронной подписи (Владелец СКП ЭП) – субъект информационного обмена, которому в установленном Федеральным законом № 63-ФЗ «Об электронной подписи» порядке Подчиненный удостоверяющий центр выдал СКП ЭП.

Внеплановая смена Ключей электронной подписи – смена ключевой пары, вызванная компрометацией Ключа ЭП, выходом из строя ключевого носителя или изменением данных СИО, содержащихся в СКП ЭП.

Единая система идентификации и аутентификации – федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

Запрос на выдачу Сертификата ключа проверки электронной подписи (Запрос на выдачу СКП ЭП) – электронное сообщение определенного формата и синтаксиса, созданное в соответствии со стандартом PKCS#10 и содержащее значение ключа проверки электронной подписи и другую необходимую информацию для создания СКП ЭП.

Запрос на отзыв Сертификата ключа проверки электронной подписи (Запрос на отзыв СКП ЭП) – электронное сообщение определенного формата и синтаксиса, содержащее необходимую информацию для отзыва СКП ЭП.

Заявление на выдачу Сертификата ключа проверки электронной подписи (Заявление на выдачу СКП ЭП) – документ, сформированный на основании Запроса на выдачу СКП ЭП Клиента-юридического лица. Заявление на выдачу СКП ЭП подписывается СИО - уполномоченным представителем ЮЛ.

Идентификация Субъекта информационного обмена (Идентификация СИО) – процесс мероприятий по установлению сведений о СИО и их проверке, осуществляемых в соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи».

Инфраструктура открытых ключей – интегрированный набор служб и приложений, основанных на технологии асимметричной криптографии, которая обеспечивает функции управления ключами проверки ЭП и СКП ЭП.

Клиенты – физические лица, юридические лица (за исключением кредитных организаций), использующие ЭП для выполнения операций с цифровым рублем.

Ключ проверки электронной подписи (Ключ проверки ЭП) – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП (далее – проверка ЭП).

Ключ электронной подписи (Ключ ЭП) – уникальная последовательность символов, предназначенная для создания ЭП.

Ключ электронной подписи ПУЦ (Ключ ЭП ПУЦ) – ключ ЭП соответствующий ключ проверки ЭП которого содержится в Сертификате ПУЦ. Используется Банком для подписания ПУЦ СКП ЭП и САС, выдаваемых и публикуемых ПУЦ.

Ключевая пара (криптографические ключи) – ключ ЭП и соответствующий ему ключ проверки ЭП.

Ключевая информация – Ключ ЭП, Ключ проверки ЭП, СКП ЭП.

Ключевой носитель – мобильное устройство или отчуждаемый носитель информации, предназначенный для размещения ключевой информации, используемой для выполнения криптографических процедур зашифрования, расшифрования, формирования и проверки ЭП.

Компрометация ключа электронной подписи – установленный факт раскрытия ключа ЭП неуполномоченным лицам или подозрение на раскрытие ключа ЭП неуполномоченным лицам; утрата доверия к тому, что используемая ключевая информация обеспечивает подлинность, защищенность и безопасность информации. К фактам, которые могут рассматриваться как компрометация (или подозрение на компрометацию) ключа ЭП, относятся следующие события:

- утрата ключевых носителей;
 - утрата ключевых носителей с последующим их обнаружением;
 - увольнение работника, имевшего доступ к ключу ЭП и (или) к ключевому носителю, на который записан указанный ключ ЭП;
 - нарушение правил хранения и уничтожения (после окончания срока действия) ключа ЭП;
 - возникновение подозрений на утечку конфиденциальной информации или ее искажение;
 - нарушение целостности упаковки ключевых носителей и (или) печати на хранилище, где хранились данные носители;
 - случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что выход из строя произошел в результате несанкционированных действий злоумышленника).
- Первые из четырех перечисленных выше событий должны трактоваться как безусловная компрометация ключа ЭП, остальные события – как подозрение на компрометацию ключа ЭП.

Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с требованиями законодательства Российской Федерации.

Конфликтная ситуация – ситуация, при которой у СИО возникает необходимость разрешить вопросы признания или непризнания факта подписания ЭП электронных документов, целостности электронного документа и/или подлинности ЭП, которой подписан электронный документ. Порядок разбора конфликтных ситуаций приведен в Приложении 1 к настоящему Регламенту.

Несанкционированный доступ к информации – доступ к информации, нарушающий установленные правила разграничения доступа в результате случайных или преднамеренных действий СИО или других субъектов, с использованием штатных аппаратных, аппаратно-программных, программных средств автоматизированной системы;

Объектный идентификатор (OID)– идентификатор объекта (поля) в СКП ЭП.

Платформа Цифрового рубля (Платформа ЦР) – информационная система, посредством которой взаимодействуют оператор платформы, участники платформы и пользователи платформы в целях совершения операций с цифровыми рублями. Оператором Платформы ЦР является Банк России, участниками Платформы ЦР являются Банки, предоставляющие своим клиентам доступ к Платформе ЦР. Пользователями Платформы ЦР являются физические лица, юридические лица, включая индивидуальных предпринимателей или физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, которым предоставлен доступ к Платформе ЦР.

Подтверждение владения ключом электронной подписи – получение ПУЦ доказательства того, что СИО владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному СИО в Запросе на выдачу СКП ЭП.

Подчиненный удостоверяющий центр (ПУЦ) – комплекс аппаратно-программных средств и организационно-технических мероприятий Банка, предназначенный для осуществления деятельности, предусмотренной Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», включая функции по регистрации СИО в ПУЦ, созданию, выдаче и отзыву СКП ЭП СИО, а также иные функции, предусмотренные настоящим Регламентом.

Представитель Клиента – физическое лицо, уполномоченное клиентом, являющимся юридическим лицом, на регистрацию в качестве СИО в Реестрах ПУЦ и получение таким СИО СКП ЭП.

Простая электронная подпись (ПЭП) – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Рабочий день ПУЦ – период с 10 часов 00 минут до 17 часов 00 минут с понедельника по пятницу по времени часовой зоны г. Москвы, за исключением нерабочих праздничных и выходных дней согласно законодательству Российской Федерации.

Регистрация СИО – внесение в Реестры ПУЦ регистрационной информации о СИО.

Реестры ПУЦ – набор документов ПУЦ в электронной и/или бумажной форме, включающий следующую информацию:

- реестр запросов на регистрацию СИО в ПУЦ;
- реестр зарегистрированных СИО;
- реестр запросов на СКП ЭП;
- реестр запросов на отзыв СКП ЭП;
- реестр СКП ЭП;
- реестр отозванных СКП ЭП;
- реестр изготовленных САС.

Отзыв сертификата ключа проверки электронной подписи – аннулирование сертификата или прекращение действия сертификата Подчиненным Удостоверяющим Центром до окончания срока действия данного сертификата.

Сертификат ключа проверки электронной подписи (СКП ЭП) – электронный документ или документ на бумажном носителе, выданные ПУЦ СИО и подтверждающие принадлежность ключа проверки ЭП владельцу СКП ЭП.

Сертификат ПУЦ – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром Банка России для ПУЦ и подтверждающий принадлежность ключа проверки ЭП ПУЦ.

Список аннулированных сертификатов (САС) – список серийных номеров сертификатов ключей проверки ЭП, которые были отозваны, а также информация о датах и причинах отзыва данных сертификатов.

Средство ЭП – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций:

- создание ЭП;
- проверка ЭП;
- создание ключа ЭП и ключа проверки ЭП.

Субъект информационного обмена (СИО) – присоединившиеся к настоящему Регламенту Клиент или Представитель Клиента, сведения о которых, включены в Реестры ПУЦ.

Усиленная неквалифицированная ЭП – электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа ЭП;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

- создана с использованием средств ЭП.

Система дистанционного банковского обслуживания для физических лиц (Система ДБО ФЛ) - система Enter.UniCredit для физических лиц в АО ЮниКредит Банке.

Система электронного документооборота для юридических лиц (Система ЭДО ЮЛ) - система Business.Online для юридических лиц и индивидуальных предпринимателей в АО ЮниКредит Банке.

Участники электронного взаимодействия – Платформа ЦР, ПУЦ и СИО, осуществляющие обмен информацией в электронной форме.

ФСБ России – Федеральная служба безопасности Российской Федерации.

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в ЭДО.

Электронный образ документа – это копия бумажного документа, преобразованного в электронную форму путём сканирования или фотографирования с сохранением его реквизитов.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. В рамках настоящего Регламента Клиентами и ПУЦ применяется усиленная неквалифицированная ЭП для операций с цифровым рублем.

1.2. Сокращения

PKCS – Public Key Cryptography Standarts.

Банк – АО ЮниКредит Банк.

Владелец СКП ЭП – Владелец сертификата ключа проверки электронной подписи.

ЕСИА – Единая система идентификации и аутентификации.

ПУЦ – Подчиненный удостоверяющий центр.

СИО – субъект информационного обмена.

СКП ЭП – сертификат ключа проверки электронной подписи.

СЦР – счет цифрового рубля.

Федеральный закон № 63-ФЗ – Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

ФП – финансовый посредник.

ЦР – цифровой рубль.

ЭП – электронная подпись.

2. Общие положения

2.1. В данном документе описан Регламент Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России.

2.2. Настоящий Регламент разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров, а также нормативно-правовыми актами Банка России, регулирующими порядок проведения операций на Платформе ЦР, включая требования к обеспечению защиты информации при осуществлении действий на Платформе ЦР и операций с ЦР.

2.3. Настоящий Регламент определяет условия предоставления услуг ПУЦ, включая права, обязанности и ответственность СИО и ПУЦ, порядок регистрации СИО в ПУЦ, порядок создания, смены и отзыва СКП ЭП.

2.4. ПУЦ осуществляет свою деятельность на территории Российской Федерации на основании имеющейся у Банка лицензии, выданной Федеральной службой безопасности Российской Федерации, на осуществление видов деятельности, связанных с предоставлением услуг удостоверяющего центра:

- Лицензия на осуществление распространения шифровальных (криптографических) средств (за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных ФСБ России) и информационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ по техническому обслуживанию шифровальных (криптографических) средств, предоставления услуг по шифрованию и имитозащите информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.

2.5. Адрес Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России для почтовой переписки: 119034, Россия, Москва, Пречистенская наб. д. 9.

3. Присоединение к Регламенту

3.1. Настоящий Регламент является договором присоединения в соответствии со ст. 428 Гражданского кодекса Российской Федерации.

3.2. Присоединение к Регламенту Клиента - физического лица осуществляется путем направления таким Клиентом - физическим лицом Запроса на выдачу СКП ЭП посредством Системы ДБО ФЛ. С момента подачи Запроса на выдачу СКП ЭП Клиентом - физическим лицом такой Клиент считается присоединившимся к настоящему Регламенту и становится Стороной Регламента.

3.3. Присоединение к Регламенту Клиента - юридического лица (за исключением кредитных организаций) осуществляется путем присоединения представителя юридического лица и направления таким Представителем Запроса на выдачу СКП ЭП посредством Системы ЭДО ЮЛ. С момента подачи Запроса на выдачу СКП ЭП представителем Клиента, такой Клиент считается присоединившимся к настоящему Регламенту и становится Стороной Регламента.

3.4. Клиент/СИО обязуется обеспечить ознакомление с требованиями настоящего Регламента, изменениями и/или дополнениями, внесенными Банком в настоящий Регламент, и их неукоснительное соблюдение.

4. Публикация Регламента

4.1. Настоящий Регламент размещается в электронной форме в виде файла формата PDF на официальном сайте Банка в сети Интернет по адресу: <https://www.unicreditbank.ru>.

4.2. В случае прекращения действия настоящего Регламента, в том числе в случае, предусмотренном разделом 6 настоящего Регламента соответствующая информация размещается на официальном сайте Банка в сети Интернет по адресу: <https://www.unicreditbank.ru>.

5. Порядок внесения изменений в Регламент

5.1. Внесение изменений и/или дополнений в настоящий Регламент (в том числе, утверждение Банком новой редакции настоящего Регламента) производится в порядке, предусмотренным настоящим разделом, и в соответствии с действующим законодательством Российской Федерации.

5.2. Изменения и дополнения в настоящий Регламент вносятся Банком в одностороннем порядке.

5.3. Банк не несет ответственности за возможные убытки Клиента/СИО, причиненные его неосведомленностью в случае, если Банк надлежащим образом выполнил свои обязательства.

5.4. Любые изменения и/или дополнения в настоящий Регламент, в том числе утвержденная Банком новая редакция настоящего Регламента, с момента вступления их в силу равно распространяются на всех лиц, присоединившихся к настоящему Регламенту, в том числе присоединившихся к настоящему Регламенту ранее даты вступления изменений в силу, если иное не предусмотрено соответствующими изменениями и/или дополнениями в настоящий Регламент.

5.5. Уведомление Клиента/СИО о внесении изменений в Регламент осуществляется способом, указанным в разделе «Публикация Регламента».

6. Прекращение деятельности ПУЦ

6.1. Деятельность ПУЦ может быть прекращена в случаях и порядке, установленных действующим законодательством Российской Федерации. При этом информация, внесенная в Реестры ПУЦ, уничтожается или передаётся лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность, в соответствии с порядком, установленным действующим законодательством Российской Федерации. При прекращении деятельности ПУЦ настоящий Регламент прекращает свое действие.

6.2. Официальное уведомление о прекращении деятельности ПУЦ и прекращении действия настоящего Регламента осуществляется путем публикации текста официального уведомления на официальном сайте Банка в сети Интернет по адресу: <https://www.unicreditbank.ru>.

7. Основные функции ПУЦ

7.1. ПУЦ предназначен для оказания услуг по созданию, выдаче и отзыву СКП ЭП, а также для предоставления иных услуг, соответствующих положениям Федерального закона № 63-ФЗ «Об электронной подписи». В рамках своей деятельности ПУЦ осуществляет следующие функции:

- регистрирует СИО;
- создает и выдает СКП ЭП по обращению СИО;
- отзывает СКП ЭП, выданные ПУЦ;
- устанавливает сроки действия СКП ЭП;
- ведет реестр СКП ЭП и реестр отозванных СКП ЭП, в том числе включающий в себя информацию, содержащуюся в выданных ПУЦ СКП ЭП, и информацию о датах прекращения действия или отзыва СКП ЭП и об основаниях таких прекращений или отзыва;
- устанавливает порядок ведения Реестров ПУЦ и порядок доступа к ним, а также обеспечивает доступ участников электронного взаимодействия к информации, содержащейся в реестре СКП ЭП в соответствии с требованиями Федерального закона № 63-ФЗ;
- проверяет уникальность ключей проверки ЭП в реестре СКП ЭП;
- устанавливает порядок проверки подлинности ЭП;
- изготавливает и публикует актуальный САС, обеспечивает возможность свободного доступа участников электронного взаимодействия к САС;

- осуществляет по обращениям участников электронного взаимодействия процедуру разбора конфликтных ситуаций, включающую проверку подлинности ЭП на основании Заявления на проверку подлинности электронной подписи в электронном документе¹;
- осуществляет подтверждение владения СИО ключом ЭП, соответствующим ключу проверки ЭП, указанному СИО для получения СКП ЭП;
- предъявляет требования по обеспечению информационной безопасности при использовании ключей ЭП и средств ЭП в процессе осуществления юридически значимого электронного документооборота между Клиентом и ПУЦ.

7.2. Порядок проверки подлинности ЭП состоит в проверке одновременного соблюдения следующих условий:

- СКП ЭП является действительным на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного СКП ЭП, если момент подписания электронного документа не определен;
- имеется положительный результат проверки принадлежности владельцу СКП ЭП данной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. При этом проверка осуществляется с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ, и с использованием сертификата лица, подписавшего электронный документ;
- ЭП используется в отношениях, определенных областями действия, указанными в СКП ЭП лица, подписывающего электронный документ.

8. Условия конфиденциальности

8.1. Конфиденциальная информация:

- Ключ ЭП, связанный с СКП ЭП СИО, является конфиденциальной информацией данного СИО. ПУЦ не осуществляет хранение ключей ЭП СИО.
- Реестры ПУЦ, за исключением реестра СКП ЭП и реестра отозванных СКП ЭП, являются конфиденциальной информацией ПУЦ и относятся к коммерческой тайне.

¹ Приложение 3 к настоящему Регламенту.

- Отчет о проведении технической экспертизы по проверке подлинности ЭП в электронном документе, выполненной по Заявлению на проверку подлинности электронной подписи в электронном документе², является конфиденциальной информацией ПУЦ.
 - Персональные данные СИО и информация о Клиенте, от лица которого действуют СИО, ставшая известной ПУЦ в силу его деятельности и не подлежащая включению в СКП ЭП, являются конфиденциальной информацией.
- 8.2. Информация, не относящаяся к конфиденциальной информации:
- Настоящий Регламент, сведения, включаемые в СКП ЭП и САС, издаваемые ПУЦ.
- 8.3. Предоставление конфиденциальной информации ПУЦ:
- ПУЦ имеет право раскрывать конфиденциальную информацию третьим лицам исключительно в порядке и случаях, установленных законодательством Российской Федерации.

9. Права и обязанности ПУЦ

9.1. Обязанности ПУЦ

- 9.1.1. Использовать для создания ключа ЭП ПУЦ и формирования ЭП, исключительно сертифицированные ФСБ России средства ЭП.
- 9.1.2. Использовать ключ ЭП ПУЦ исключительно для подписи выдаваемых ПУЦ СКП ЭП и публикуемых САС.
- 9.1.3. Принимать меры по защите ключа ЭП ПУЦ от несанкционированного доступа.
- 9.1.4. Обеспечивать уникальность серийных номеров создаваемых СКП ЭП СИО.
- 9.1.5. Проверять уникальность значений ключей проверки ЭП в реестре СКП ЭП.
- 9.1.6. Информировать СИО об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки. Информирование СИО осуществляется путем размещения «Руководства по обеспечению безопасности использования ключей электронной подписи и средств электронной подписи» в Приложении 4 к настоящему Регламенту.
- 9.1.7. Обеспечивать актуальность информации, содержащейся в реестре СКП ЭП, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.
- 9.1.8. Предоставлять в соответствии с требованиями Федерального закона № 63-ФЗ «Об электронной подписи» безвозмездно доступ к информации, содержащейся в реестре СКП ЭП, реестре отозванных СКП ЭП.

² Приложение 3 к настоящему Регламенту.

- 9.1.9. Отказать СИО в создании СКП ЭП в случае, если не было подтверждено то, что СИО владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному СИО для получения СКП ЭП.
- 9.1.10. Обеспечивать конфиденциальность созданных ПУЦ ключей ЭП.
- 9.1.11. Отказать СИО в создании СКП ЭП в случае отрицательного результата проверки в реестре СКП ЭП уникальности ключа проверки ЭП, указанного СИО для получения СКП ЭП.
- 9.1.12. Соблюдать сроки отзыва СКП ЭП.
- 9.1.13. Осуществлять регистрацию СИО на основании Запросов на выдачу СКП ЭП, в соответствии с положениями, определенными настоящим Регламентом.
- 9.1.14. Обеспечивать занесение регистрационной информации СИО в Реестры ПУЦ и обеспечивать уникальность регистрационной информации, используемой для идентификации владельцев СКП ЭП.
- 9.1.15. Обеспечивать конфиденциальность регистрационной информации СИО, за исключением информации, заносимой в СКП ЭП, выдаваемые ПУЦ.
- 9.1.16. Осуществлять создание СКП ЭП СИО в соответствии с нормами, определенными настоящим Регламентом.
- 9.1.17. Обеспечивать внесение информации о созданном СКП ЭП СИО в реестр СКП ЭП не позднее указанной в нем даты начала действия такого сертификата.
- 9.1.18. Отозвать СКП ЭП СИО путем внесения записи о его отзыве в САС с указанием даты, времени внесения и причины отзыва не позднее 12 (двенадцати) часов как ПУЦ стало известно или должно было стать известно об обстоятельствах, влекущих необходимость отзыва СКП ЭП.
- 9.1.19. Уведомлять владельца СКП ЭП о фактах отзыва, принадлежащего ему СКП ЭП, путём информирования посредством Системы ДБО ФЛ в случае Клиентов-физических лиц или Системы ЭДО ЮЛ в случае Клиентов-юридических лиц.
- 9.1.20. Обеспечивать сохранность и контроль доступа к конфиденциальной информации в соответствии с действующими нормативными актами Российской Федерации.
- 9.1.21. Гарантировать конфиденциальность сведений, полученных в связи с исполнением своих обязательств по настоящему Регламенту, в течение срока хранения документов, установленного законодательством об архивном деле в Российской Федерации.
- 9.1.22. Поддерживать во всех технических и программных средствах ПУЦ единое системное время, соответствующее времени часовой зоны г. Москвы, с точностью до 01 минуты.
- 9.1.23. Отозвать СКП ЭП СИО в случаях когда:
- не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате,

- установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи,
- вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию,
- на основании Запроса на отзыв СКП ЭП, поданного СИО посредством Системы ДБО ФЛ или Системы ЭДО ЮЛ,
- в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ним нормативными правовыми актами.

9.2. Права ПУЦ

9.2.1. Отказать в предоставлении услуг по регистрации СИО в ПУЦ в случае нарушения указанным СИО требований настоящего Регламента, с указанием причин отказа.

9.2.2. Отказать в предоставлении услуг по созданию СКП ЭП СИО в случае нарушения указанным СИО требований настоящего Регламента с указанием причин отказа.

9.2.3. Отказать СИО в предоставлении услуг по созданию СКП ЭП в случае, если использованное для формирования запроса на СКП ЭП средство ЭП не поддерживается ПУЦ.

9.2.4. Отозвать СКП ЭП СИО в случаях когда:

- установлен факт компрометации соответствующего ключа ЭП, в том числе и без соответствующего заявления со стороны владельца СКП ЭП,
- в случае если ПУЦ стало достоверно известно о прекращении действия документа, на основании которого выдан СКП ЭП,
- если установлено, что СКП ЭП содержит сведения, утратившие свою достоверность в связи с изменением данных СИО или Клиента,
- если установлено, что в результате технической ошибки СКП ЭП содержит недостоверные или неполные сведения.

10. Права и обязанности СИО

10.1. Права СИО

10.1.1. Применять ключи ЭП и СКП ЭП, владельцем которых указанный СИО является, для формирования ЭП под электронными документами при осуществлении защищенного юридически значимого электронного документооборота и обмена информацией в рамках взаимодействия с Платформой ЦР.

10.1.2. Для СКП ЭП, выданного в форме электронного документа, получить по запросу копию СКП ЭП на бумажном носителе, заверенную ПУЦ.

10.1.3. Получать Сертификат ПУЦ и использовать его для проверки ЭП ПУЦ в СКП ЭП, выданных ПУЦ.

10.1.4. Получать актуальный САС ПУЦ и применять его для проверки статуса СКП ЭП, выданных ПУЦ, и для проверки ЭП электронных документов.

10.1.5. Обращаться в соответствии с настоящим Регламентом³ в ПУЦ для проверки подлинности ЭП в электронных документах, подписанных с использованием СКП ЭП, выданных ПУЦ.

10.1.6. Обращаться в соответствии с настоящим Регламентом в ПУЦ для отзыва СКП ЭП, в течение срока действия данного СКП ЭП.

10.2. Обязанности СИО

10.2.1. Формировать ключи ЭП согласно требованиям, предъявляемым к средствам криптографической защиты информации.

10.2.2. Соблюдать условия и порядок использования ключей ЭП и средств ЭП.

10.2.3. Обеспечивать конфиденциальность своего ключа ЭП, принимать все возможные меры для предотвращения утраты, раскрытия, искажения и несанкционированного использования ключа ЭП, его компрометации.

10.2.4. Применять для формирования ЭП только действующий не скомпрометированный ключ ЭП.

10.2.5. Не применять свой ключ ЭП, если стало известно или имеются подозрения, что данный ключ ЭП используется или использовался ранее другими лицами.

10.2.6. Немедленно обратиться в соответствии с настоящим Регламентом в ПУЦ с запросом на отзыв своего СКП ЭП при наличии оснований полагать, что ключ ЭП скомпрометирован.

10.2.7. Не использовать ключ ЭП, связанный с СКП ЭП запрос на отзыв которого подан в ПУЦ, с момента подачи такого запроса.

10.2.8. Не использовать ключ ЭП, связанный с СКП ЭП, который отозван. Использование отозванного СКП ЭП не влечет юридических последствий, за исключением тех, которые связаны с его отзывом.

10.2.9. Применять свой ключ ЭП исключительно в отношениях, определенных областями действия, указанными в связанном с данным ключом ЭП СКП ЭП.

11. Ответственность сторон

11.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту стороны несут ответственность в порядке, предусмотренном действующим законодательством Российской Федерации.

³ См. Приложение 3 к настоящему Регламенту.

11.2. ПУЦ несет ответственность за убытки, возникшие вследствие или в связи с использованием СИО СКП ЭП, выданного ПУЦ только в случае, если указанные убытки возникли вследствие компрометации ключа ЭП ПУЦ. СИО понимает и принимает риски, связанные с использованием ЭП и средств ЭП, включая компрометацию ключа ЭП и несанкционированное использование ключа ЭП, при ненадлежащем соблюдении СИО мер безопасности.

11.3. Ответственность сторон, не урегулированная настоящим Регламентом, регулируется в соответствии с действующим законодательством Российской Федерации.

11.4. ПУЦ не несет ответственности за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникших в связи с этим убытков, в случаях:

- если ПУЦ обоснованно полагался на сведения, указанные в Запросе на выдачу СКП ЭП или Запросе на отзыв СКП ЭП;
- вследствие компрометации ключа ЭП СИО.

12. Сроки действия криптографических ключей и СКП ЭП

12.1. Сроки действия криптографических ключей и Сертификата ПУЦ⁴

12.1.1. Срок действия ключа ЭП ПУЦ составляет 36 (тридцать шесть) календарных месяцев. Срок действия Сертификата ПУЦ, соответствующего ключу ЭП ПУЦ, составляет 18 (восемнадцать) лет.

12.1.2. В течении 15 (пятнадцати) месяцев ключ ЭП ПУЦ используется для подписания СКП ЭП СИО и САС ПУЦ, остальное время ключ ЭП ПУЦ используется для подписания САС ПУЦ.

12.1.3. Плановая смена криптографических ключей ПУЦ осуществляется в порядке, предусмотренном Регламентом взаимодействия Финансового посредника и Банка России при управлении криптографическими ключами Платформы Цифрового рубля.

12.2. Сроки действия ключей и СКП ЭП СИО

12.2.1. Срок действия ключа ЭП СИО составляет 15 (пятнадцать) календарных месяцев.

12.2.2. Срок действия СКП ЭП, соответствующего ключу ЭП СИО, составляет 6 лет 3 месяца (75 месяцев), и определяется по атрибутам сертификата «Действителен с» - «Действителен по».

12.2.3. СКП ЭП прекращает свое действие:

- в связи с истечением установленного срока его действия,

⁴ Перечень, структура и правила заполнения полей сертификатов ключей электронной подписи, сертификатов ключей шифрования и список отозванных сертификатов регламентированы в документе Центрального Банка Российской Федерации «Платформа Цифрового рубля. Правила заполнения полей сертификата». В случае актуализации документа «Платформа Цифрового рубля. Правила заполнения полей сертификата» перечень, структура и правила заполнения полей сертификатов ключей электронной подписи, сертификатов ключей шифрования и список отозванных сертификатов также подлежат изменению согласно вновь утвержденному документу ЦБ РФ.

- на основании Запроса на отзыв СКП ЭП, подаваемого в порядке, предусмотренном разделом 16 настоящего Регламента,
- в случае прекращения деятельности ПУЦ без перехода его функций другим лицам,
- в случае если ПУЦ стало достоверно известно о прекращении действия документа, на основании которого выдан СКП ЭП, в том числе прекращении действия в отношении Договора использования Системы ДБО ФЛ или Системы ЭДО ЮЛ в части операций с цифровыми рублями, включая расторжение договора счета цифрового рубля,
- в иных случаях, установленных Федеральным законом от № 63-ФЗ «Об электронной подписи», в также согласно требованиям законодательства Российской Федерации.

13. Хранение СКП ЭП в ПУЦ

13.1. Хранение СКП ЭП в Реестре ПУЦ осуществляется в течение всего срока деятельности ПУЦ, если более короткий срок не установлен нормативными правовыми актами.

14. Регистрация СИО в Реестре ПУЦ

14.1. Под регистрацией СИО в Реестрах ПУЦ понимается внесение регистрационных данных СИО в информационную систему ПУЦ.

14.2. Регистрация СИО в Реестрах ПУЦ осуществляется на основании поданного СИО Запроса на выдачу СКП ЭП в Системе ДБО ФЛ или Системе ЭДО ЮЛ, содержащего регистрационные данные Клиента, а в случае Клиента ЮЛ также и его представителя.

14.3. Инициирование регистрации СИО в Реестрах ПУЦ осуществляется после успешной идентификации СИО.

15. Порядок создания и выдачи СКП ЭП СИО

Сертификат ключа проверки электронной подписи создаётся средствами ПУЦ на основе сведений, указанных в Запросе на СКП ЭП. Порядок создания и выдачи СКП ЭП СИО зависит от технологии создания сертификата, предоставляемой Клиенту Системой ДБО ФЛ или Системой ЭДО ЮЛ.

15.1. Порядок создания и выдачи СКП ЭП Клиента-Физического лица

15.1.1. Клиент-Физическое лицо (СИО) в целях получения доступа к функционалу счета цифрового рубля при помощи Системы ДБО ФЛ проходит идентификацию и аутентификацию в ЕСИА.

15.1.2. После успешной аутентификации СИО в ЕСИА Система ДБО ФЛ получает из ЕСИА данные СИО: фамилия, имя, отчество (при наличии), ИНН, СНИЛС, данные основного документа, удостоверяющего личность СИО.

15.1.3. Система ДБО ФЛ с использованием инфраструктуры Банка осуществляет проверку соответствия данных СИО, содержащихся в информационных системах Банка, данным полученным из ЕСИА в результате его аутентификации в ЕСИА.

15.1.4. После подтверждения соответствия данных, СИО самостоятельно с использованием функциональности Системы ДБО ФЛ и входящего в её состав средства электронной подписи, создает ключ электронной подписи, ключ проверки электронной подписи и формирует Запрос на выдачу СКП ЭП.

15.1.5. Запрос на выдачу СКП ЭП, содержащий ключ проверки ЭП и данные СИО, с использованием функциональности Системы ДБО ФЛ передаётся по организованным каналам информационно-технологического взаимодействия в ПУЦ.

15.1.6. ПУЦ осуществляет контроли Запроса на выдачу СКП ЭП:

- проверяет целостность Запроса на выдачу СКП ЭП,
- проверяет уникальность указанного в Запросе на выдачу СКП ЭП ключа проверки ЭП в Реестре сертификатов ПУЦ,
- осуществляет форматно-логический контроль структуры и состава Запроса на выдачу СКП ЭП.

15.1.7. В случае положительного результата контролей ПУЦ, на основании полученного Запроса на выдачу СКП ЭП, создаёт СКП ЭП и передаёт его по организованным каналам информационно-технологического взаимодействия в Систему ДБО ФЛ.

15.1.8. После получения СКП ЭП в Системе ДБО ФЛ СИО получает возможность использовать ключ ЭП и СКП ЭП для подписания электронных документов усиленной неквалифицированной электронной подписью в рамках операций с ЦР и взаимодействия с Платформой цифрового рубля с использованием Системы ДБО ФЛ.

15.1.9. В случае если результат проверки сведений СИО, содержащихся в информационных системах Банка, не соответствует сведениям, полученным из ЕСИА, или результат контролей Запроса на выдачу СКП ЭП отрицательный ПУЦ не создаёт СИО СКП ЭП.

15.2. Порядок создания и выдачи СКП ЭП Клиента-юридического лица

15.2.1. Представитель Клиента-ЮЛ (СИО) в целях получения доступа к функционалу счета цифрового рубля самостоятельно с использованием функциональности Системы ЭДО ЮЛ и средств электронной подписи, размещённых на его автоматизированном рабочем месте, создаёт ключ электронной подписи, ключ проверки электронной подписи и формирует Запрос на выдачу СКП ЭП.

15.2.2. Запрос на выдачу СКП ЭП, содержащий ключ проверки ЭП, данные Клиента и его представителя, с использованием Системы ЭДО ЮЛ передаётся по организованным каналам информационно-технологического взаимодействия в ПУЦ.

15.2.3. На основании сформированного Запроса на выдачу СКП ЭП в Системе ЭДО ЮЛ формируется Заявление на выдачу СКП ЭП. Форма Заявления на выдачу СКП ЭП приведена в Приложении 2 к настоящему Регламенту.

15.2.4. Заявление на выдачу СКП ЭП может быть подано СИО в ПУЦ как в форме бумажного документа, так и в форме электронного образа бумажного документа, подписанного квалифицированной электронной подписью СИО.

15.2.5. СИО с использованием функциональности Системы ЭДО ЮЛ распечатывает Заявление на выдачу СКП ЭП.

15.2.6. В случае подачи Заявления на выдачу СКП ЭП в форме документа на бумажном носителе СИО:

- подписывает его собственноручной подписью и предоставляет лично в офис АО ЮниКредит Банка,
- Подчинённый Удостоверяющий центр осуществляет идентификацию СИО при личном присутствии СИО по основному документу, удостоверяющему личность гражданина Российской Федерации - паспорту гражданина Российской Федерации.

15.2.7. В случае подачи Заявления на выдачу СКП ЭП в дистанционной форме СИО предоставляет в инфраструктуру Банка по организованным каналам информационно-технологического взаимодействия подписанный своей квалифицированной электронной подписью электронный образ Заявления на выдачу СКП ЭП на бумажном носителе. В этом случае идентификация СИО осуществляется без его личного присутствия по квалифицированной электронной подписи СИО.

15.2.8. При предоставлении Заявления на выдачу СКП ЭП в форме документа, подписанного квалифицированной электронной подписью СИО:

- для подписания электронной подписью должны использоваться средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи».
- должен применяться ключ электронной подписи, соответствующий квалифицированный сертификата ключа проверки ЭП которого действует на момент подписания.

15.2.9. После успешной идентификации СИО в ПУЦ инициируется создание СКП ЭП. ПУЦ осуществляет контроли Запроса на выдачу СКП ЭП:

- проверяет целостность Запроса на выдачу СКП ЭП,

- проверяет уникальность указанного в Запросе на выдачу СКП ЭП ключа проверки ЭП в Реестре сертификатов ПУЦ,
- осуществляет форматно-логический контроль структуры и состава Запроса на выдачу СКП ЭП.

15.2.10. В случае положительного результата контролей ПУЦ, на основании полученного Запроса на выдачу СКП ЭП, создаёт СКП ЭП и передаёт его по организованным каналам информационно-технологического взаимодействия в Систему ЭДО ЮЛ.

15.2.11. После получения СКП ЭП в Системе ЭДО ЮЛ СИО получает возможность использовать ключ ЭП и СКП ЭП для подписания электронных документов усиленной неквалифицированной электронной подписью в рамках операций с ЦР и взаимодействия с Платформой цифрового рубля на своём автоматизированном рабочем месте в Системе ЭДО ЮЛ.

15.2.12. В случае если результат контролей Запроса на выдачу СКП ЭП отрицательный или при ошибках в оформлении Заявления на выдачу СКП ЭП, а также если идентификация СИО не была осуществлена в течении 30 календарных дней с даты формирования Запроса на СКП ЭП (включая дату формирования Запроса), ПУЦ отказывает СИО в выдаче СКП ЭП. Информирование СИО об отказе в выдаче СКП ЭП осуществляется при помощи Системы ЭДО ЮЛ.

16. Отзыв СКП ЭП СИО

16.1. Отзыв СКП ЭП, выданного ПУЦ, осуществляется на основании Запроса на отзыв СКП ЭП, подаваемого в электронной форме с использованием Системы ДБО ФЛ или Системы ЭДО ЮЛ.

16.2. Запрос на отзыв СКП ЭП передаётся в ПУЦ по организованным каналам информационно-технологического взаимодействия.

16.3. В случае принятия ПУЦ положительного решения об отзыве сертификата Подчиненный Удостоверяющий центр включает сведения об отозванном СКП ЭП в САС в течение 12 часов с момента как ему стало известно или должно было стать известно об обстоятельствах, повлекших отзыв СКП ЭП.⁵

16.4. Датой и временем отзыва СКП ЭП признается дата и время внесения информации о сертификате, который был отозван, в САС.

16.5. Официальным уведомлением о факте отзыва СКП ЭП является опубликование САС, который содержит сведения об отозванном сертификате.

⁵ В соответствии с документом Регламент взаимодействия Финансового посредника и Банка России при управлении криптографическими ключами Платформы Цифрового рубля (вторая редакция) п. 4.2. ФП производит выпуск САС ПУЦ ФП не реже одного раза в 7 дней и в случае отзыва сертификата пользователя ПлЦР.

16.6. Временем опубликования САС признаётся время его создания.

17. Смена криптографических ключей ПУЦ

17.1. Плановая смена криптографических ключей (ключа ЭП и соответствующего ему ключа проверки ЭП) ПУЦ выполняется через 1 год (12 месяцев) и не позднее, чем через 15 (пятнадцать) календарных месяцев после начала действия ключа ЭП ПУЦ⁶.

17.2. Плановая смена ключа ЭП ПУЦ не влечет за собой необходимости смены ключей ЭП и СКП ЭП субъектов информационного обмена.

17.3. Внеплановая смена ключей ЭП ПУЦ выполняется в случае установления факта компрометации ключа ЭП ПУЦ или подозрения на наличие такого факта. Сертификат ключа проверки электронной подписи ПУЦ в таком случае отзывается. Все СКП ЭП, подписанные с использованием скомпрометированного ключа ЭП ПУЦ, также считаются отозванными.

17.4. Уведомление САО о компрометации ключа ЭП ПУЦ осуществляется посредством размещения данной информации на сайте Банка в сети Интернет по адресу: <https://www.unicreditbank.ru> и рассылки соответствующего сообщения при наличии данной функциональности в Системе ДБО ФЛ или Системе ЭДО ЮЛ.

17.5. Все подписанные с использованием скомпрометированного ключа ЭП ПУЦ и действовавшие на момент компрометации ключа ЭП ПУЦ СКП ЭП САО подлежат внеплановой смене в порядке, установленном настоящим Регламентом.

18. Смена криптографических ключей САО

18.1. Смена криптографических ключей САО выполняется в случае истечения срока действия ключа ЭП САО, установленного факта компрометации ключа электронной подписи САО, в случае выхода из строя ключевого носителя, в случае изменения данных САО, содержащихся в СКП ЭП, а также в иных случаях, предусмотренных настоящим Регламентом.

18.2. Смена СКП ЭП САО осуществляется согласно разделу 15 (пятнадцать) настоящего Регламента.

18.3. В случае установленного факта компрометации криптографических ключей САО, в случае выхода из строя ключевого носителя, а также в случае изменения данных САО, в СКП ЭП, САО необходимо предварительно отозвать СКП ЭП согласно разделу 16 настоящего Регламента.

⁶ Актуальный срок указан в документе Правила заполнения полей сертификата.

19. Порядок действий владельца СКП ЭП при компрометации его ключа ЭП

19.1. В случае подозрения о компрометации ключа ЭП владелец СКП ЭП самостоятельно принимает решение о факте компрометации принадлежащего ему ключа ЭП.

19.2. В случае компрометации или подозрения о компрометации ключа ЭП СИО отзывает действие СКП ЭП, соответствующего скомпрометированному ключу, в порядке, установленном разделом 16 настоящего Регламента.

20. Содержание и форма СКП ЭП

20.1. СКП ЭП, выдаваемый Клиенту-физическому лицу, содержит серийный номер сертификата, даты начала и окончания срока действия, идентификатор алгоритма, значение ключа проверки электронной подписи, а также информацию в поле «Владелец» сертификата:

- ID Пользователя ПлЦР (соответствующий идентификатор Пользователя ПлЦР согласно Альбому ЭС),
- ID ФП (соответствующий идентификатор ФП, Участника ПлЦР, у которого обслуживается Пользователь ПлЦР согласно Альбому ЭС) ,
- ID СЦР Пользователя ПлЦР (соответствующий идентификатор СЦР на ПлЦР согласно Альбому ЭС),
- фамилия, имя, отчество (если имеется),
- СНИЛС,
- дополнительную информацию по требованиям ПлЦР.

20.2. СКП ЭП, выдаваемый представителю Клиента-юридического лица, содержит серийный номер сертификата, даты начала и окончания срока действия, идентификатор алгоритма, значение ключа проверки электронной подписи, а также информацию в поле «Владелец» сертификата:

- ID Пользователя ПлЦР (соответствующий идентификатор Пользователя ПлЦР согласно Альбому ЭС),
- ID ФП (соответствующий идентификатор ФП, Участника ПлЦР, у которого обслуживается Пользователь ПлЦР согласно Альбому ЭС) ,
- ID СЦР Пользователя ПлЦР (соответствующий идентификатор СЦР на ПлЦР согласно Альбому ЭС),

- наименование Клиента-ЮЛ,
- местонахождение Клиента-ЮЛ,
- фамилия, имя, отчество (если имеется) представителя ЮЛ
- дополнительную информацию по требованиям ПлЦР.

21. Хранение материалов

21.1. Информация, внесенная в реестр СКП ЭП и реестр отозванных СКП ЭП, подлежит хранению в течение всего срока деятельности ПУЦ в соответствии с Федеральным законом "Об электронной подписи" от 06.04.2011 N 63-ФЗ».

21.2. Документы на бумажных носителях, в том числе и выданные ПУЦ копии СКП ЭП в виде документов на бумажном носителе, хранятся в порядке и в течение сроков, установленных законодательством Российской Федерации в отношении клиентской документации.

21.3. Документы, срок архивного хранения которых закончился, подлежат уничтожению в соответствии с действующей процедурой в Банке.

Приложение 1.

к Регламенту Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России

Порядок разбора конфликтных ситуаций

1. Общие положения

1.1. Область применения

1.1.1. Порядок разбора конфликтных ситуаций (далее – Порядок) определяет порядок разбора конфликтных ситуаций в случаях:

- отказа СИО от факта подписания ЭП электронного документа (авторства над электронным документом, подписанным ЭП);
- отказа СИО от содержания электронного документа, подписанного его ЭП (целостности и/или подлинности электронного документа, подписанного с использованием ЭП).

1.1.2. Настоящий Порядок применяется исключительно для разрешения конфликтных ситуаций, связанных с применением в Системе ДБО ФЛ или Системе ЭДО ЮЛ СКП ЭП, выданных ПУЦ. Вопросы урегулирования споров и разногласий между СИО, участвующими в информационном обмене без применения услуг ПУЦ, и/или СИО и организациями, возникшие по иным основаниям, не рассматриваются в настоящем Порядке и подлежат разрешению сторонами в соответствии с иными соглашениями и нормативными документами.

1.1.3. В настоящем Порядке применяются термины в соответствии с терминологией Регламента Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России (далее – Регламент ПУЦ).

1.2. Основания для разбора конфликтных ситуаций

1.2.1. Разбор конфликтных ситуаций, перечисленных в пункте 1.1.1 настоящего Порядка, заключается в доказательстве принадлежности или непринадлежности ЭП на электронном документе со всеми его реквизитами, авторство или целостность и подлинность которого оспаривается, конкретному СИО, а также в подтверждении наличия или отсутствия искажений в электронном документе, подписанном ЭП указанного СИО.

1.2.2. Порядок разбора конфликтных ситуаций, перечисленных в пункте 1.1.1 настоящего Порядка, основан на действующих нормативно-правовых актах Российской Федерации, а также математических свойствах процесса формирования и проверки ЭП, функции хэширования и алгоритма криптографического преобразования, реализованных в сертифицированных средствах ЭП, применяемых в автоматизированных банковских, информационных и телекоммуникационных системах Банка для защиты электронных документов.

1.2.3. Математические свойства криптографических алгоритмов, описываемых указанными ниже в данном пункте российскими государственными стандартами таковы, что гарантируют невозможность подделки значения ЭП под электронным документом любым лицом, не обладающим ключом ЭП:

- ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
- ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

1.2.4. Соответствие используемых средств ЭП перечисленным выше государственным стандартам Российской Федерации подтверждается наличием у указанных средств действующих сертификатов ФСБ России.

1.2.5. Для доказательства факта принадлежности ЭП под электронным документом, авторство и/или целостность и/или подлинность которого оспаривается, конкретному СИО, а также с целью подтверждения наличия или отсутствия искажений в электронном документе, подписанном ЭП, используется специальное программное обеспечение Банка, которое применяется для выполнения необходимых проверок и документирования результатов.

2. Порядок разбора конфликтных ситуаций

2.1. В соответствии с данной процедурой подлежат разбору конфликтные ситуации, связанные с отказом СИО от факта подписания им электронного документа или непризнанием СИО целостности и подлинности документа, подписанного его ЭП. Разбор конфликтной ситуации является процедурой проверки подлинности ЭП СИО под документом, авторство и/или целостность и/или подлинность, которого оспаривается.

2.2. Проверка подлинности ЭП конкретного СИО под электронными документами, используемыми в рамках взаимодействия с платформой цифрового рубля, осуществляется ПУЦ.

2.3. Процедура проверки подлинности ЭП под электронным документом проводится на основании Заявления на проверку подлинности электронной подписи в электронном документе (далее – Заявление), выполненного на бумажном носителе, а также с использованием Системы ДБО ФЛ или Системы ЭДО ЮЛ, по форме Приложения 3 к Регламенту ПУЦ и поданного в любое отделение Банка СИО в течение рабочего дня Банка.

2.4. Заявление должно содержать следующую информацию:

- дату и время подачи Заявления;
- идентификационные данные СИО, ЭП которого под электронным документом требует проверки;
- дату и время формирования ЭП под электронным документом;

- дату и время событий, на момент наступления которых требуется установить подлинность ЭП под электронным документом. В случае наличия в ЭП штампа времени, сформированного Службой штампов времени, дата и время формирования ЭП, указанные в штампе времени ЭП, считаются достоверными.

В остальных случаях бремя доказывания достоверности даты и времени формирования ЭП в электронном документе возлагается на СИО, подавшего Заявление. Обязательными приложениями к Заявлению должны являться и должны быть предоставлены СИО на отчуждаемом носителе информации следующие сведения:

- электронный документ с ЭП (электронный документ отдельно от подписи или электронный документ в одном файле с подписью), авторство и (или) целостность и подлинность которого оспаривается, либо реквизиты электронного документа с ЭП, идентифицирующие его в Системе ДБО ФЛ или Системе ЭДО ЮЛ (наименование электронного документа, порядковый номер электронного документа в ИС, дата создания электронного документа);
- СКП ЭП, с использованием которого требуется осуществить проверку ЭП электронного документа, авторство и (или) целостность и подлинность которого оспаривается.

2.5. СИО при подаче в Банк Заявления сообщает предпочитаемый канал связи для уведомления СИО о дате, времени и месте проведения технической экспертизы по проверке подлинности ЭП под электронным документом (далее – Экспертиза).

2.6. Срок проведения процедуры Экспертизы по проверке подлинности ЭП под электронным документом составляет не менее 10 (десяти) рабочих дней и не более 20 (двадцати) рабочих дней с момента подачи Заявления в Банк.

2.7. О назначенной дате, времени и месте проведения Экспертизы Банк уведомляет СИО.

2.8. Банк осуществляет процедуру проверки подлинности ЭП под электронным документом в назначенное время в присутствии СИО. Неявка СИО, извещенного о дате, времени и месте проведения Экспертизы в соответствии с пунктом 2.5 настоящего Порядка, не препятствует проведению Экспертизы.

2.9. При проведении процедуры Экспертизы Банк осуществляет следующие действия:

2.9.1. Проверяет действительность ЭП под оспариваемым электронным документом с использованием файлов самого документа, его ЭП и СКП ЭП предполагаемого автора документа, предоставленных СИО, на момент времени, указанный в его Заявлении, с распечаткой протокола проверки ЭП, а также проверку подлинности СКП ЭП предполагаемого автора электронного документа на момент времени, указанный в Заявлении.

2.9.2. При положительном результате проведенных проверок (в протоколе проверки ЭП сформирована запись о действительности ЭП, то есть подтверждении корректности оспариваемого

электронного документа, и при отсутствии СКП ЭП отправителя оспариваемого электронного документа в САС ПУЦ на рассматриваемый момент времени) предоставляет СИО СКП ЭП и выписку из реестра выданных СКП ЭП СИО на момент времени формирования ЭП, указанный в Заявлении.

2.9.3. Осуществляет посимвольное сравнение значений полей СКП ЭП, предоставленного СИО, и значений полей СКП ЭП, распечатанного из реестра выданных СКП ЭП.

2.10. Положительный результат проверки подлинности ЭП под электронным документом доказывает авторство, целостность и подлинность оспариваемого документа.

2.11. Результатом проведения Экспертизы является заключение, составленное в двух экземплярах.

Заключение Банка содержит:

- дату, время и место проведения проверки;
- состав лиц, осуществлявший проверку;
- основание для проведения проверки;
- результаты проверки;
- обоснование выводов результатов проверки.

Один экземпляр заключения хранится в Банке. Второй экземпляр заключения передается СИО под подпись. В случае отсутствия СИО в момент проведения Экспертизы, экземпляр заключения направляется в его адрес с использованием услуг АО «Почта России» заказным письмом по адресам, имеющимся в распоряжении Банка.

Приложение 2.

к Регламенту Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России

Заявление на выдачу сертификата ключа проверки неквалифицированной электронной подписи (юридические лица)

Настоящим, владелец ключа электронной подписи

Фамилия, имя, Отчество			
Тип документа		Дата выдачи	
Серия		Номер	
Орган, выдавший документ			
Компания			
Клиентский номер			

обращается в Удостоверяющий центр АО ЮниКредит Банка, подчиненный подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России, за получением неквалифицированного сертификата ключа проверки электронной подписи, содержащего следующие сведения:

Ключ проверки электронной подписи	значение ключа проверки ЭП
Наименование средства электронной подписи	CryptoPro CSP
Владелец (DN)	
C	RU
O	ID Пользователя ⁵
CN	ID ФП ⁶
L	CBDC
OU	ID СЦР Пользователя ПлЦР ⁷
STREET	1. наименование ЮЛ 2. место нахождения юридического лица – клиента ПлЦР 3. Фамилия, Имя, Отчество физического лица, уполномоченного представителя ЮЛ
GN	Пользователь ПлЦР

Приложением к данному заявлению и его неотъемлемой частью является запрос на выдачу неквалифицированного сертификата ключа проверки электронной подписи, переданный в Удостоверяющий центр АО ЮниКредит Банка в электронной форме с использованием системы Business.Online.

=====

⁵ ID Пользователя – соответствующий идентификатор Пользователя ПлЦР согласно Альбому ЭС

⁶ ID ФП – соответствующий идентификатор ФП, Участника ПлЦР, у которого обслуживается Пользователь ПлЦР согласно Альбому ЭС

⁷ ID СЦР Пользователя ПлЦР – соответствующий идентификатор СЦР на ПлЦР согласно Альбому ЭС

Подписывая настоящее заявление, владелец ключа электронной подписи в соответствии со ст. 428 ГК РФ полностью и безусловно присоединяется к «Регламенту Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России» (далее «Регламент»), условия которого определены и опубликованы на сайте АО ЮниКредит Банка, и подтверждает полное принятие условий Регламента и всех его положений.

Заполняется в случае идентификации владельца ключа электронной подписи при его личном присутствии:

- владелец ключа ЭП - ФИО, дата, подпись

- сотрудник АО ЮниКредит Банка: подтвержден приём Заявления на выдачу сертификата ключа проверки электронной подписи и проведение идентификации- ФИО, дата, подпись

Приложение 3.

к Регламенту Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России

Заявление на проверку подлинности электронной подписи в электронном документе

Настоящим, _____

(фамилия, имя, отчество Субъекта информационного обмена, его место жительства)

_____ серия _____ № _____, выдан «__» _____ 20__ г.

(наименование документа, удостоверяющем личность)

(кем выдан)

просит проверить подлинность электронной подписи в электронном документе на основании следующих данных:

- **файла сертификата ключа проверки электронной подписи подписанта отмеченного электронного документа;**
- **файла оспариваемого электронного документа с ЭП/реквизитов оспариваемого электронного документа;**
- **даты и времени, на момент наступления которых требуется подтвердить подлинность электронной подписи: «__» _____ 20__ г. __ ч. __ мин. по московскому времени.**

(если дата и время не указаны, то подлинность электронной подписи устанавливается на дату принятия заявления Банком).

Прошу уведомить меня о дате, времени и месте проведения технической экспертизы по проверке подлинности ЭП под электронным документом следующим способом: _____.

Субъект информационного обмена: _____

(подпись)

(расшифровка

подписи)

«__» _20__ г.

Заполняется Банком:

Настоящим подтверждаю, что заявление на проверку подлинности электронной подписи в электронном документе принято, личность

(фамилия, имя, отчество заявителя)

идентифицирована, сведения, указанные в заявлении, проверены.

Отказано¹

(указать причину отказа в принятии заявления)

Ответственный работник АО ЮниКредит Банка должность

¹ Заполняется в случае отказа в принятии заявления.

М.П.*(подпись)* *(расшифровка подписи)*

«_____» _____ 20__ г.

Приложение 4.

к Регламенту Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России

Руководство по обеспечению безопасности использования ключей электронной подписи и средств электронной подписи

1. Общие положения

Настоящее Руководство подготовлено в соответствии с частью 2 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и предназначено для официального информирования владельцев сертификатов ключей проверки электронной подписи, выдаваемых Удостоверяющим центром АО ЮниКредит Банка, подчиненным подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России (далее – ПУЦ), о рисках, условиях и правилах применения ЭП и средств ЭП, а также о мерах, необходимых для обеспечения безопасности использования ЭП и средств ЭП.

При использовании в правоотношениях ЭП, использовании и эксплуатации средств ЭП владельцы СКП ЭП и средств ЭП должны соблюдать требования:

- Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 № 152;
- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 09.02.2005 № 66;
- эксплуатационной документации на средства ЭП;
- Регламента Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России (далее – Регламент ПУЦ);
- настоящего Руководства.

2. Риски, связанные с использованием ЭП

К основным рискам, связанным с использованием ЭП, относятся:

2.1. Несанкционированное подписание электронного документа ЭП, которое может быть произведено в результате:

Регламент Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России

- компрометации ключа ЭП;
- подмены подписываемого электронного документа в результате работы на компьютере или мобильном устройстве вредоносного программного обеспечения.

2.2. Негативные последствия, вызванные невозможностью подписания электронного документа ЭП, обусловленной следующими событиями:

- уничтожение (удаление с ключевого носителя) ключа ЭП и (или) СКП ЭП;
- неисправность ключевого носителя, на котором хранятся ключ ЭП и (или) СКП ЭП;
- блокировка доступа к ключу ЭП, вызванная неоднократным вводом некорректного кода доступа (пароля или PIN-кода);
- физическая утрата ключевого носителя.

3. Основные меры безопасности для владельцев СКП ЭП, направленных на избежание указанных рисков

3.1. Порядок получения сертифицированных средств ЭП

3.1.1. Для ФЛ: Путем скачивания ДБО ФЛ из точки распространения на Интернет-ресурсе производителя или магазинов приложений RuStore, GooglePlay, AppStore, Huawei App Gallery. Такой способ получения средства электронной подписи является легальным только в отношении тех средств ЭП, распространение которых через сеть Интернет согласовано с ФСБ России.

Для ЮЛ и ИП:

3.1.2. На устанавливающих средствах ЭП носителях информации. Распространение устанавливающих средств ЭП носителей осуществляется лицами, имеющими лицензию ФСБ России на выполнение соответствующих видов работ и оказание услуг в отношении шифровальных (криптографических) средств.

3.2. Требования по размещению средств вычислительной техники с установленными средствами ЭП

3.2.1. При размещении стационарных средств вычислительной техники (далее – СВТ) с установленными на них средствами ЭП должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых размещены данные СВТ.

3.2.2. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны выполняться, исходя из необходимости создания условий для обеспечения сохранения конфиденциальности используемых ключей ЭП и иной конфиденциальной информации.

3.3. Требования к общесистемному и специальному программному обеспечению

3.3.1. На СВТ, предназначенных для работы со средствами ЭП, необходимо использовать только лицензионное программное обеспечение (далее – ПО).

3.3.2. На СВТ с установленными средствами ЭП не должны использоваться средства разработки ПО и отладчики.

3.3.3. Не допускается установка ОС, не предусмотренных документацией на средства ЭП либо измененных или отладочных версий ОС, указанных в документации; - не допускается установка программных средств, реализующих функции удаленного управления, администрирование, модификацию ОС и ее настроек, а также среды разработки;

- не допускается установка нескольких ОС;
- неиспользуемые ресурсы СВТ должны быть отключены (протоколы, сервисы и т.п.);
- реализованные на СВТ режимы безопасности должны быть настроены на максимальный уровень;
- зарегистрированным пользователям СВТ назначаются минимально возможные для нормальной работы права;
- предоставление минимальных прав доступа к ресурсам СВТ, включая доступ к системному реестру, файлам и каталогам, временным файлам, файлам подкачки и т.п.

3.3.4. Программное обеспечение, устанавливаемое на СВТ с установленным средством ЭП, не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других программ;
- модифицировать память, выделенную для других программ;
- передавать управление в область собственных данных и данных других программ;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- модифицировать настройки ОС;
- использовать недокументированные функции ОС.

3.4. Требования по защите от несанкционированного доступа при эксплуатации средств ЭП

Регламент Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России

При организации работ по защите ключевой информации от несанкционированного доступа необходимо руководствоваться требованиями эксплуатационной документации на соответствующее средство ЭП, а также учитывать следующие общие требования:

3.4.1. Правом доступа к СВТ с установленными средствами ЭП должны обладать только владельцы ключей ЭП, установленных на данных СВТ. Каждый СИО должен быть ознакомлен с настоящим Руководством и документацией на средства ЭП.

3.4.2. На СВТ с установленными средствами ЭП необходимо использовать средства антивирусной защиты.

3.4.3. При использовании средств ЭП необходимо использовать пароли, сформированные в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля могут присутствовать буквы в верхнем и нижнем регистрах, а также цифры;
- использование в составе символов пароля специальных символов (@, #, \$, &, *, % и т.п.) позволяет при необходимости значительно увеличить стойкость используемого пароля;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- периодичность смены пароля определяется политикой безопасности, но не должна превышать 1 (одного) календарного года.

3.4.4. Запрещается:

- оставлять без контроля СВТ, на котором установлены средства ЭП, после ввода ключевой информации либо иной конфиденциальной информации;
- использовать несертифицированные средства ЭП;
- вносить какие-либо изменения в ПО средств ЭП;
- осуществлять несанкционированное копирование ключевой информации;
- разглашать содержимое ключевой информации или передавать ключевые носители посторонним лицам, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать ключ ЭП, связанный с сертификатом ключа проверки ЭП, в отношении которого в ПУЦ зарегистрировано заявление об аннулировании.

Регламент Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России

3.4.5. Необходимо своевременно устанавливать обновления ОС и антивирусного ПО, в том числе и обновления баз данных антивирусного ПО.

3.4.6. При подключении СВТ с установленными средствами ЭП к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

3.4.7. При использовании средств ЭП на СВТ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых ОС, к ПО, в окружении которого функционируют средства ЭП, и к компонентам средств ЭП со стороны указанных сетей, рекомендуется использовать дополнительные методы и средства защиты (например, установка межсетевых экранов и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.

3.4.8. Перед началом работы со средствами ЭП необходимо изучить настоящее Руководство и эксплуатационную документацию на средства ЭП.

3.4.9. Ответственность за обеспечение конфиденциальности PIN-кода и ключа ЭП возлагается на владельца ключа ЭП.

3.5. Требования по защите от несанкционированного доступа к ключевой информации при использовании ключевых носителей

3.5.1. Создаваемые ключи ЭП должны записываться на ключевые носители, имеющее подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности. Не допускается хранение на носителе ключевой информации любой иной информации (в том числе рабочих или личных файлов). Типы ключевых носителей, которые поддерживаются применяемым средством ЭП, устанавливаются согласно технической и эксплуатационной документации на средство ЭП.

3.5.2. После получения ключевого носителя (типа Рутокен и т.п.) пользователь ЮЛ или ИП должен произвести смену предустановленных на нем PIN-кодов пользователя и администратора, используемых для аутентификации. Значения предустановленных PIN-кодов указаны в эксплуатационной документации на соответствующий ключевой носитель.

3.5.3. PIN-коды должны состоять не менее чем из 8 символов. Символы могут включать в себя как буквы и цифры, так и знаки препинания и т.п.

Регламент Удостоверяющего центра АО ЮниКредит Банка, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России

3.5.4. В ходе эксплуатации ключевого носителя рекомендуется производить смену действующих PIN-кодов с периодичностью, не превышающей 6 календарных месяцев.

3.5.5. Ключевые носители должны использоваться только владельцем ключа ЭП, размещенного на ключевом носителе, и храниться в нерабочие периоды времени в месте, исключающем возможность его бесконтрольного использования. В частности, одним из способов контроля сохранности ключей ЭП, содержащегося на ключевом носителе, является его хранение в сейфе (металлическом шкафу, колбе), опечатываемом личной печатью владельца ключа ЭП (владельца ключевого носителя).

3.5.6. Ответственность за обеспечение конфиденциальности PIN-кода и ключа ЭП возлагается на владельца ключа ЭП.

4. Действия при компрометации ключей ЭП

4.1. САО самостоятельно должен определить факт компрометации ключа ЭП, оценить значение такого события и выполнить мероприятия по локализации последствий компрометации ключа ЭП.

4.2. При компрометации ключа ЭП САО должен немедленно инициировать мероприятия по аннулированию СКП ЭП в соответствии с требованиями Регламента ПУЦ.