

Приложение 17
к Регламенту Удостоверяющего центра
АО «Россельхозбанк»
(приказ АО «Россельхозбанк» от 04.07.2024 № 1098-ОД)

**Порядок получения TLS-сертификатов, используемых в рамках взаимодействия с
Платформой ЦР, и правила по обеспечению безопасности TLS-ключей**

Содержание

1. Термины, определения и сокращения	3
2. Общие положения	4
3. Сроки действия TLS-ключей и TLS-сертификатов.....	5
4. Регистрация СИО в реестре УЦ РСХБ.....	5
5. Создание TLS-сертификата	5
6. Аннулирование TLS-сертификата	6
7. Смена TLS-ключей СИО	7
8. Порядок действий владельца TLS-сертификата при компрометации его TLS-ключа	7
9. Правила по обеспечению безопасности TLS-ключей.....	7

Приложение:

1. Заявление на выдачу TLS-сертификата Субъекта информационного обмена (для физических лиц).
2. Заявление на выдачу TLS-сертификата Субъекта информационного обмена (для юридических лиц).
3. Заявление на аннулирование TLS-сертификата Субъекта информационного обмена.
4. Информация, содержащаяся в TLS-сертификате.
5. Заявление о предоставлении TLS-сертификата на бумажном носителе.
6. Правила по обеспечению безопасности TLS-ключей.

1. Термины, определения и сокращения

Единый сервисный договор – договор о предоставлении банковских продуктов/услуг, состоящий из условий Единого сервисного договора банковского обслуживания юридических лиц (за исключением кредитных организаций), индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой (приказ АО «Россельхозбанк» от 09.10.2024 № 983-ОД), в АО «Россельхозбанк» и Заявления¹ о присоединении к Единому сервисному договору²;

Запрос на выдачу TLS-сертификата – электронное сообщение определенного формата и синтаксиса, созданное в соответствии со стандартом PKCS#10 и содержащее необходимую информацию для создания TLS-сертификата;

Запрос на аннулирование TLS-сертификата – электронное сообщение определенного формата и синтаксиса, созданное в соответствии со стандартом PKCS#10 и содержащее необходимую информацию для аннулирования TLS-сертификата;

Заявление на выдачу TLS-сертификата Субъекта информационного обмена (заявление СИО) – подписанный ПЭП СИО документ, сформированный СИО в электронном виде на основании Запроса на выдачу TLS-сертификата с использованием ИС по форме Приложения 1 или 2 к настоящему Порядку;

Заявление на аннулирование – документ на бумажном носителе, выполненный по форме Приложения 3 к настоящему Порядку, на основании которого осуществляется аннулирование TLS-сертификата;

Идентификация СИО – идентификация, проводимая Банком при личном присутствии СИО, включающая в себя установление личности СИО по основному документу, удостоверяющему личность, или без личного присутствия СИО, проводимая в ИС с использованием ПЭП СИО;

Ключевой носитель – мобильное устройство или отчуждаемый носитель информации, предназначенный для размещения ключевой информации, используемой для аутентификации владельца TLS-сертификата и создания зашифрованного канала связи с реализацией двусторонней аутентификации;

Обработка запроса на выдачу TLS-сертификата или запроса на аннулирование TLS-сертификата – совокупность действий Банка по созданию TLS-сертификата, занесению о нем сведений в реестры УЦ РСХБ или занесению сведений об аннулировании TLS-сертификата в реестры УЦ РСХБ и формированию и публикации CRL, а также уведомлению владельца TLS-сертификата о создании или аннулировании TLS-сертификата в соответствии с настоящим Порядком;

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;

Простая электронная подпись (ПЭП) – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования

¹ За исключением случая присоединения к Единому сервисному договору без оформления такого заявления, т.е. в порядке, установленном Единым сервисным договором, иными договорами, заключенными между Банком и Клиентом, в том числе в порядке, установленном п. 6.9 договора о дистанционном банковском обслуживании с использованием Системы СДБО «Интернет-Клиент»/п. 6.5 договора о дистанционном банковском обслуживании с использованием Системы «Мобильный банк».

² Приложение 4 к Единому сервисному договору банковского обслуживания юридических лиц (за исключением кредитных организаций), индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой

электронной подписи определенным лицом. В рамках настоящего Порядка применяется простая электронная подпись, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации;

Рассмотрение запроса на аннулирование TLS-сертификата – принятие Банком решения об осуществлении обработки запроса на аннулирование TLS-сертификата на основе предоставленных владельцем TLS-сертификата документов;

СКЗИ – сертифицированное средство криптографической защиты информации;

Условия ДБО ФЛ – Условия дистанционного банковского обслуживания физических лиц в АО «Россельхозбанк» с использованием системы «Интернет-банк» и «Мобильный банк», неотъемлемой частью которых является настоящий Порядок;

Условия ДБО ЮЛ – Условия дистанционного банковского обслуживания Клиента - юридического лица (за исключением кредитных организаций)/индивидуального предпринимателя/физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой с использованием системы «Банк-Клиент»/«Интернет-Клиент» или Условия дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Россельхозбанк» с использованием информационной системы «Цифровой канал обслуживания юридических лиц «Свой бизнес» в рамках Единого сервисного договора;

ЦР – Цифровой рубль.

Остальные термины и определения, применяемые в настоящем Порядке, используются в значении, определенном в Регламенте Удостоверяющего центра АО «Россельхозбанк».

2. Общие положения

2.1. Регламент Удостоверяющего центра АО «Россельхозбанк», включая Порядок получения TLS-сертификатов, используемых в рамках взаимодействия с Платформой ЦР, и правила по обеспечению безопасности TLS-ключей (далее – Порядок) являются неотъемлемой частью Условий ДБО ФЛ и Условий ДБО ЮЛ, определяют условия предоставления услуг УЦ РСХБ в части создания, смены и аннулирования TLS-сертификатов, включая права, обязанности и ответственность СИО и Банка, связанных с созданием, сменой и аннулированием TLS-сертификатов, порядок регистрации СИО в УЦ РСХБ, порядок создания, смены и аннулирования TLS-сертификатов.

2.2. Банк не взимает комиссионное вознаграждение за услуги, оказываемые УЦ РСХБ в соответствии с настоящим Порядком.

2.3. Присоединение к Клиента - физического лица к Регламенту Удостоверяющего центра АО «Россельхозбанк» и Порядку для получения TLS-сертификатов осуществляется путем направления таким Клиентом - физическим лицом Заявления СИО по форме Приложения 1 к настоящему Порядку посредством ИС. С момента приема к исполнению Заявления СИО, направленного Клиентом - физическим лицом, такой Клиент считается присоединившимся к настоящему Порядку и становится Стороной Порядка.

2.4. Присоединение Клиента - юридического лица (за исключением кредитных организаций)/индивидуального предпринимателя/физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой к Регламенту Удостоверяющего центра АО «Россельхозбанк» для получения TLS-сертификатов, осуществляется путем присоединения Клиента - юридического лица/индивидуального предпринимателя/физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой к Условиям ДБО ЮЛ. С момента присоединения Клиента - юридического лица/индивидуального предпринимателя/физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой, к Условиям ДБО ЮЛ, Клиент считается

присоединившимся к Регламенту Удостоверяющего центра АО «Россельхозбанк» и на него распространяется настоящий Порядок.

2.5. Настоящий Порядок 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, а также при осуществлении операций с ЦР.

2.6. Порядок регистрации СИО в реестрах УЦ РСХБ, получения и аннулирования TLS-сертификатов, используемых в рамках взаимодействия с Платформой ЦР, и правила по обеспечению безопасности TLS-ключей определяются в рамках настоящего Порядка.

3. Сроки действия TLS-ключей и TLS-сертификатов

3.1. Сроки действия TLS-ключей и TLS-сертификатов СИО.

3.1.1. Максимальный срок действия TLS-ключа и TLS-сертификатов СИО составляет 15 (пятнадцать) календарных месяцев.

Началом срока действия TLS-ключа СИО считается дата и время начала действия TLS-сертификата, связанного с данным TLS-ключом, выданного УЦ РСХБ, определяемые по атрибуту TLS-сертификата «Действителен с».

3.1.2. TLS-сертификат прекращает свое действие:

- в связи с истечением установленного срока его действия;
- на основании Запроса на аннулирование TLS-сертификата или Заявления на аннулирование, подаваемого в соответствии с требованиями п. 6 настоящего Порядка;
- в случае прекращения деятельности УЦ РСХБ без перехода его функций другим лицам;
- в случае если УЦ РСХБ стало достоверно известно о прекращении действия документа, на основании которого выдан TLS-сертификат, в том числе о прекращении действия договорных отношений с Банком;
- в случае прекращения деятельности УЦ РСХБ;
- в иных случаях в соответствии с законодательством Российской Федерации.

3.2. Хранение TLS-сертификатов в УЦ РСХБ.

Хранение TLS-сертификата в реестре УЦ РСХБ осуществляется в течение всего срока деятельности УЦ РСХБ, если более короткий срок не установлен нормативными правовыми актами.

4. Регистрация СИО в реестре УЦ РСХБ

Инициирование регистрации СИО в реестрах УЦ РСХБ осуществляется таким СИО с использованием ИС после успешной идентификации СИО.

5. Создание TLS-сертификата

5.1. Запрос на выдачу TLS-сертификата в электронной форме формируется и подается СИО с использованием функционала ИС после успешной идентификации СИО.

5.2. СИО с использованием ИС:

- формирует на основании Запроса на выдачу TLS-сертификата Заявление СИО³ в электронной форме;
- иницирует передачу Заявления СИО в УЦ РСХБ.

5.3. УЦ РСХБ принимает к исполнению Заявление СИО и в случае принятия положительного решения создает TLS-сертификат на основе Запроса на выдачу TLS-сертификата и Заявления СИО и включает его в реестры УЦ РСХБ не позднее 3 (трех) рабочих

³ Приложение 1 или Приложение 2 к настоящему Порядку, включающее сведения из Запроса на выдачу TLS-сертификата, сформированного в соответствии с п. 4 настоящего Порядка.

дней УЦ РСХБ, следующих за рабочим днем Банка, в течение которого Заявление СИО было получено Банком.

5.4 В случае если Заявление СИО не прошло положительную проверку, УЦ РСХБ отказывает в выдаче TLS-сертификата.

5.5. СИО может использовать TLS-сертификат, выпущенный согласно п. 5.3 настоящего Порядка, после подтверждения согласия с содержимым TLS-сертификата с использованием ИС⁴.

5.6. TLS-сертификат на бумажном носителе может быть выдан владельцу TLS-сертификата на основании Заявления о предоставлении TLS-сертификата на бумажном носителе, выполненного по форме Приложения 5 к настоящему Порядку. Банк передает TLS-сертификат его владельцу не позднее 10 (десяти) рабочих дней УЦ РСХБ, следующих за рабочим днем Банка, в который соответствующее заявление поступило в Банк.

6. Аннулирование TLS-сертификата

6.1. Аннулирование TLS-сертификата, выданного УЦ РСХБ, осуществляется на основании:

- Запроса на аннулирование TLS-сертификата, подаваемого в электронной форме с использованием ИС⁵;
- Заявления на аннулирование на бумажном носителе, подаваемого СИО в Банк при личном присутствии в двух экземплярах, выполненного по форме Приложения 3 к настоящему Порядку.

6.2. Запрос на аннулирование в электронной форме

6.2.1. СИО инициирует аннулирование TLS-сертификата с использованием ИС.

6.2.2. ИС направляет Запрос на аннулирование TLS-сертификата в УЦ РСХБ.

6.2.3. УЦ РСХБ, при положительном результате рассмотрения Запроса на аннулирование TLS-сертификата, аннулирует TLS-сертификат СИО.

6.2.4. ИС информирует СИО об аннулировании TLS-сертификата в порядке, предусмотренном Условиями ДБО ФЛ и Единым сервисным договором.

6.3. Заявление на аннулирование на бумажном носителе

6.3.1. Банк, при приеме от СИО Заявления на аннулирование на бумажном носителе, выполняет идентификацию СИО при его личном присутствии, устанавливая личность с использованием документа, удостоверяющего личность⁶.

6.3.2. Банк, в процессе идентификации СИО в день подачи Заявления на аннулирование, принимает решение о приеме или отказе в приеме указанного Заявления на аннулирование.

6.3.3. Банк может отказать в приеме Заявления на аннулирование в случае отсутствия у СИО документа, удостоверяющего личность, а также в случае ненадлежащего оформления Заявления на аннулирование.

6.3.4. В случае принятия Банком положительного решения об аннулировании TLS-сертификата, Банк включает сведения об аннулированном TLS-сертификате в CRL, издаваемого УЦ РСХБ, не позднее 1 (одного) рабочего дня УЦ РСХБ, следующего за рабочим днем Банка, в течение которого Заявление на аннулирование было принято Банком.

6.3.5. В случае если Заявление на аннулирование не прошло проверку, СИО может быть отказано в аннулировании TLS-сертификата. В таком случае Банк направляет СИО официальное уведомление с указанием причины отказа способом, определенным Условиями

⁴ Подтверждение согласия СИО с содержимым выпущенного TLS-сертификата осуществляется таким СИО с использованием доступного в ИС способа подтверждения согласия с содержимым TLS-сертификата, визуализированного в ИС по форме Приложения 4 к настоящему Порядку.

⁵ Возможность применения данного метода определяется договорными отношениями и при наличии в ИС соответствующего функционала.

⁶ Паспорт или иной документ, удостоверяющий личность в соответствии с законодательством Российской Федерации.

ДБО ФЛ и Единым сервисным договором, не позднее 1 (одного) рабочего дня УЦ РСХБ, следующего за рабочим днем Банка, в течение которого Заявление на аннулирование было принято Банком.

6.4. Датой аннулирования TLS-сертификата признается дата публикации CRL, содержащего сведения о TLS-сертификате, запрос на аннулирование которого был подан СИО.

7. Смена TLS-ключей СИО

7.1. Смена TLS-ключей СИО выполняется при плановой смене, в случае истечения срока действия TLS-сертификата СИО, при компрометации или подозрении на компрометацию TLS-ключей и (или) пароля для доступа к хранилищу TLS-ключей, при возникновении технических причин, а также в случаях необходимости обновления программного обеспечения, предназначенного для вычисления значения хэш-функции⁷, подтверждения авторства, целостности и обеспечения конфиденциальности электронных документов, а также в случае изменения данных СИО, содержащихся в TLS-сертификате.

7.2. Смена TLS-сертификата СИО осуществляется согласно разделу 5 настоящего Порядка.

7.2.1. В случае возникновения причин, указанных в п. 7.1 настоящего Порядка, за исключением истечения срока действия TLS-сертификата, СИО необходимо предварительно аннулировать TLS-сертификат в порядке, установленном разделом 6 настоящего Порядка.

8. Порядок действий владельца TLS-сертификата при компрометации его TLS-ключа

8.1. В случае подозрения о компрометации TLS-ключа владелец TLS-сертификата самостоятельно принимает решение о факте компрометации принадлежащего ему TLS-ключа.

8.2. В случае компрометации или подозрения на компрометацию TLS-ключа СИО аннулирует действие TLS-сертификата, соответствующего скомпрометированному TLS-ключу, в порядке, установленном п. 6 настоящего Порядка.

9. Правила по обеспечению безопасности TLS-ключей

9.1. Владелец TLS-сертификата обязан руководствоваться основными требованиями к обращению с ключевым носителем, изложенными в Договоре счета цифрового рубля между оператором платформы ЦР и пользователем платформы ЦР и требованиями Приложения 6 к настоящему Порядку.

⁷ Хэш-функция – функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим свойствам: по данному значению функции сложно вычислить исходные данные, отображаемые в это значение; для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в то же значение функции; сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение.