

Приложение 16  
к Регламенту Удостоверяющего центра  
АО «Россельхозбанк»  
(приказ АО «Россельхозбанк» от \_\_.\_\_.2025 № \_\_\_\_-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.....	5
3. Сроки действия TLS-ключей и TLS-сертификатов.....	5
4. Регистрация СИО в реестре УЦ РСХБ.....	6
5. Создание TLS-сертификата.....	6
6. Аннулирование TLS-сертификата .....	7
7. Смена TLS-ключей СИО.....	8
8. Порядок действий владельца TLS-сертификата при компрометации его TLS-ключа....	8
9. Правила по обеспечению безопасности TLS-ключей.....	8

### 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 08.10.2018 № 983-ОД), в АО «Россельхозбанк» и Заявления о присоединении к Единому сервисному договору<sup>1</sup>;

**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 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

<sup>1</sup> 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



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 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 с предоставлением в Банк подписанного собственноручной подписью СИО Согласия на обработку персональных данных<sup>2</sup>.

### **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 СИО<sup>3</sup> в электронной форме;
- инициирует 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 дней УЦ РСХБ, следующих за рабочим днем Банка, в течение которого Заявление СИО было получено Банком.

<sup>2</sup> По форме Приложения 8 к Регламенту Удостоверяющего центра АО «Россельхозбанк».

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



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 ИС<sup>4</sup>.

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 ИС<sup>5</sup>;

- Заявления на аннулирование на бумажном носителе, подаваемого СИО/Представителем Клиента 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/Представителя Клиента Заявления на аннулирование на бумажном носителе, выполняет идентификацию СИО/Представителя Клиента при его личном присутствии, устанавливая личность с использованием документа, удостоверяющего личность<sup>6</sup>.

6.3.2. Банк, в процессе идентификации СИО/Представителя Клиента 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/Представителя Клиента 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-сертификата 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/Представителю Клиента может быть отказано в аннулировании TLS-сертификата. В таком случае Банк направляет СИО/Представителю Клиента официальное уведомление с указанием причины отказа способом, определенным Условиями ДБО ФЛ и Единым

<sup>4</sup> 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.

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

<sup>6</sup> Паспорт или иной документ, удостоверяющий личность в соответствии с законодательством Российской Федерации.



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-функции<sup>7</sup>, 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 на компрометацию 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 разделом 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.

---

<sup>7</sup> 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.



**Заявление на выдачу TLS-сертификата Субъекта информационного обмена  
(физические лица)**

Настоящим, \_\_\_\_\_  
(фамилия, имя, отчество физического лица, его место жительства)  
серия \_\_\_\_\_ № \_\_\_\_\_, выдан «\_\_» \_\_\_\_\_ 20\_\_ г.  
(наименование документа, удостоверяющего личность)  
\_\_\_\_\_  
(кем выдан)  
\_\_\_\_\_  
(номер СНИЛС)  
\_\_\_\_\_  
(номер мобильного телефона)

просит на  
основании \_\_\_\_\_  
(документ, являющийся основанием для регистрации)

зарегистрировать себя в реестрах УЦ РСХБ и изготовить TLS-сертификат в соответствии с  
указанными данными:

**Сведения о запросе на сертификат:**

**Субъект запроса на сертификат:**

C=RU  
O=g.ru.cbrdc.prt.fi.1ac1614c-90fa-46a4-bce7-c5abb8a50c73  
CN=<Фамилия, имя и отчество (если имеется) клиента ПлЦР>  
L=CBDCTLS  
SNILS=<Страховой номер индивидуального лицевого счета в системе обязательного  
пенсионного страхования у клиента ПлЦР >

**Ключ проверки электронной подписи:**

Алгоритм ключа: ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1)  
Параметры: 30 13 06 07 2A 85 03 02 02 24 00 06 08 2A 85 03 07 01 01 02 02  
Значение: 0440 CC90 2079 7F3B 39B6 174F BC1B 353E 7BA3 2563 5AA9 2185 1C72 D4C9  
C4C7 2704 64CE 0758 2D76 6E7C 71FC 54E0 2995 D94B A9C3 145B 9ED9 4D50 9E04  
7F52 F74A C555 5996

(Место для ПЭП Субъекта  
информационного обмена)

Подписанием настоящего заявления,

\_\_\_\_\_  
(фамилия, имя, отчество физического лица, его место жительства)  
присоединяется в Регламенту Удостоверяющего центра АО «Россельхозбанк» в соответствии  
со ст. 428 ГК РФ.



*(Место для ПЭП Субъекта информационного обмена)*

---

**Заполняется Банком:**

Подтвержден приём Заявления на выдачу TLS-сертификата Субъекта информационного обмена и проведение идентификации Субъекта информационного обмена.

*(Место для штампа ЭП Банка)*



**Заявление на выдачу TLS-сертификата Субъекта информационного обмена  
(юридические лица)**

Настоящим, \_\_\_\_\_  
(фамилия, имя, отчество физического лица, его место жительства)  
серия \_\_\_\_\_ № \_\_\_\_\_, выдан «\_\_» \_\_\_\_\_ 20\_\_ г.  
(наименование документа, удостоверяющего личность)  
\_\_\_\_\_  
(кем выдан)  
\_\_\_\_\_  
(номер СНИЛС)  
\_\_\_\_\_  
(номер мобильного телефона)  
являющийся представителем \_\_\_\_\_  
(наименование и местонахождение юридического лица)

просит на  
основании \_\_\_\_\_  
(документ, являющийся основанием для регистрации)

зарегистрировать себя в реестрах УЦ РСХБ и изготовить TLS-сертификат в соответствии с  
указанными данными:

**Сведения о запросе на сертификат:**

**Субъект запроса на сертификат:**

C=RU  
O=g.ru.cbrdc.prt.fi.1ac1614c-90fa-46a4-bce7-c5abb8a50c73  
CN= <Фамилия, имя и отчество (если имеется) клиента ПлЦР, Наименование  
юридического лица>  
L=CBDCTLS  
SNILS=<Страховой номер индивидуального лицевого счета в системе обязательного  
пенсионного страхования у клиента ПлЦР >

**Ключ проверки электронной подписи:**

Алгоритм ключа: ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1)  
Параметры: 30 13 06 07 2A 85 03 02 02 24 00 06 08 2A 85 03 07 01 01 02 02  
Значение: 0440 CC90 2079 7F3B 39B6 174F BC1B 353E 7BA3 2563 5AA9 2185 1C72  
D4C9 C4C7 2704 64CE 0758 2D76 6E7C 71FC 54E0 2995 D94B A9C3 145B 9ED9 4D50  
9E04 7F52 F74A C555 5996

(Место для ПЭП Субъекта  
информационного обмена)

---

**Заполняется Банком:**

Подтвержден приём Заявления на выдачу TLS-сертификата Субъекта  
информационного обмена и проведение идентификации Субъекта информационного обмена.



*(Место для штампа ЭП Банка)*



### Информация, содержащаяся в TLS-сертификате

Номер сертификата:

Срок действия:

Сведения в сертификате:

1.

Владелец (DN):

Страна (C) = RU;

Организация (O) = <ID Пользователя>,

где ID Пользователя – соответствующий идентификатор Пользователя ПлЦР согласно Альбому ЭС;

Имя (CN) = <ID ФП>,

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

Область применения (L) = CBDC;

Подразделение (OU) = <ID Кошелька Пользователя ПлЦР>,

где ID Кошелька Пользователя ПлЦР – соответствующий идентификатор кошелька на ПлЦР согласно Альбому ЭС.

2.

X509v3 расширенная область применения ключа:

<BaseOID>.3.1 - для ФЛ/ФЛ-СЗ;

<BaseOID>.3.2 - для ЮЛ;

<BaseOID>.3.3 - для Клиента с прямым доступом.

3.

X509v3 Альтернативное имя Владельца:

Фамилия:

<Фамилия, имя и отчество (если имеется) клиента ПлЦР> - для ФЛ/ФЛ-СЗ;

<Наименование и место нахождения юридического лица - клиента ПлЦР> - для ЮЛ и Клиентов с прямым доступом;

Организация: Пользователь ПлЦР, обслуживающийся у ФП <ID ФП>,

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

4.

Область применения ключа: ЭП, Неотрекаемый, Согласование ключей.

5.

Срок действия сертификата: 6 лет 3 месяца (75 месяцев).

6.

Срок действия криптографического ключа: 1 год 3 месяца (15 месяцев).

Подписывая настоящий документ, СИО:

1. Выражает согласие с содержанием получаемого TLS-сертификата;

2. Подтверждает ознакомление и согласие с требованиями Регламента Удостоверяющего центра АО «Россельхозбанк» (далее – Регламент), опубликованного на официальном сайте Банка <https://www.rshb.ru> в разделе Информация об услугах - Удостоверяющий центр, и полное принятие условий Регламента и всех его положений.

3. Подтверждает получение правил по обеспечению безопасности TLS-ключей.

Дата:



**Заявление о предоставлении TLS-сертификата  
на бумажном носителе**

г. \_\_\_\_\_

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Настоящим,

\_\_\_\_\_ (фамилия, имя, отчество физического лица, его место жительства)  
серия \_\_\_\_\_ № \_\_\_\_\_, выдан « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.  
(наименование документа, удостоверяющего личность)

\_\_\_\_\_ (кем выдан),

являющийся представителем<sup>1</sup>

\_\_\_\_\_,  
(наименование и местонахождение юридического лица)  
действующий на основании \_\_\_\_\_,

Просит выдать TLS-сертификат на бумажном носителе.

**Владелец TLS-сертификата**

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(расшифровка подписи)

**Заполняется Банком**

Заявление зарегистрировано в Банке « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Ответственный работник АО «Россельхозбанк»

должность \_\_\_\_\_

\_\_\_\_\_  
(подпись) (расшифровка подписи)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

М.П.

<sup>1</sup> Применимо для клиентов – юридических лиц



## **Правила по обеспечению безопасности TLS-ключей**

### **1. Общие положения**

Правила по обеспечению безопасности TLS-ключей (далее – Правила) предназначены для информирования владельцев TLS-сертификатов, выдаваемых Удостоверяющим центром АО «Россельхозбанк», о рисках, условиях и правилах применения TLS-ключей и СКЗИ, а также о мерах, необходимых для обеспечения безопасности TLS-ключей и СКЗИ.

При использовании в правоотношениях TLS-ключей, эксплуатации СКЗИ СНО 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 СКЗИ;
- Регламента Удостоверяющего центра АО «Россельхозбанк»;
- настоящих Правил.

### **2. Риски, связанные с использованием TLS-ключей**

К основным рискам, связанным с использованием TLS-ключей, относятся:

2.1. Несанкционированный доступ (далее – НСД) к проведению операций с ЦР, который может быть осуществлен в результате компрометации TLS-ключа;

2.2. Негативные последствия, вызванные невозможностью доступа к операциям с ЦР, обусловленной следующими событиями:

- уничтожение (удаление с ключевого носителя) TLS-ключа и (или) TLS-сертификата;
- неисправность ключевого носителя, на котором хранятся TLS-ключ и (или) TLS-сертификат;
- блокировка доступа к TLS-ключу, вызванная неоднократным вводом некорректного пароля к хранилищу криптографических ключей в Программном модуле Банка России (далее – хранилище криптографических ключей), кода доступа к ключевому носителю;
- физическая утрата ключевого носителя.

### **3. Основные меры безопасности для владельцев TLS-сертификатов, направленных на избежание указанных рисков**

#### **3.1. Требования к общесистемному и специальному программному обеспечению.**

3.1.1. На ключевых носителях необходимо использовать только лицензионное программное обеспечение (далее – ПО).

3.1.2. На ключевых носителях не должны использоваться средства разработки ПО и отладчики.

3.1.3. Не допускается установка операционных систем (далее – ОС), не предусмотренных эксплуатационной документацией на СКЗИ, либо измененных или отладочных версий ОС;



- не допускается установка программных средств, реализующих функции удаленного управления, администрирования, модификации ОС и ее настроек, а также среды разработки;
- не допускается установка нескольких ОС;
- неиспользуемые ресурсы ключевых носителей должны быть отключены (протоколы, сервисы и т.п.);
- реализованные на ключевых носителях режимы безопасности должны быть настроены на максимальный уровень;
- пользователям ключевых носителей назначаются минимально возможные для нормальной работы права.

3.1.4. Программное обеспечение, устанавливаемое на ключевые носители, 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.

### **3.2. Требования по защите от несанкционированного доступа при эксплуатации СКЗИ.**

При организации работ по защите ключевой информации от НСД необходимо руководствоваться требованиями эксплуатационной документации на СКЗИ, а также учитывать следующие общие требования:

3.2.1. Правом доступа к ключевым носителям должны обладать только владельцы TLS-сертификатов. Каждый СИО должен быть ознакомлен с настоящими Правилами и эксплуатационной документацией на СКЗИ.

3.2.2. На ключевых носителях необходимо использовать средства антивирусной защиты.

3.2.3. Операции с хранилищем криптографических ключей, требующие обращения к TLS-ключам СИО, должны быть защищены паролем. Пароль к хранилищу криптографических ключей должен задаваться СИО при первом обращении к программному модулю Банка России. Длина пароля должна быть не менее 8 и не более 32 символов, и может содержать латинские буквы в верхнем и нижнем регистре, цифры и спецсимволы: | \ / . , < > ; " ' { } [ ] \_ - = + () \* & ? ^ % \$ # @ ! ` ~. Срок действия пароля — 6 календарных месяцев.

3.2.4. Запрещается:

- оставлять без контроля ключевые носители после ввода пароля от хранилища криптографических ключей либо иной конфиденциальной информации;
- использовать несертифицированные СКЗИ;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- осуществлять копирование ключевой информации, содержащейся на ключевом носителе;
- разглашать содержимое ключевой информации, пароли к хранилищу криптографических ключей, коды доступа к ключевому носителю или передавать ключевые носители посторонним лицам, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать TLS-ключ, связанный с TLS-сертификатом, в отношении которого в УЦ РСХБ зарегистрировано заявление об аннулировании.

3.2.5. Необходимо своевременно устанавливать обновления ОС и антивирусного ПО,



в том числе и обновления баз данных антивирусного ПО.

3.2.6. При подключении ключевых носителей 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.

3.2.7. При использовании ключевых носителей, подключенных к общедоступным сетям связи, с целью исключения возможности НСД к системным ресурсам используемых ОС, к ПО, в окружении которого функционируют ключевые носители, и к компонентам ключевых носителей со стороны указанных сетей, рекомендуется использовать дополнительные методы и средства защиты.

3.2.8. Перед началом работы со СКЗИ необходимо изучить настоящие Правила и эксплуатационную документацию на СКЗИ.

3.2.9. Ответственность за обеспечение конфиденциальности ключевой информации, паролей к хранилищу криптографических ключей и кодов доступа к ключевому носителю возлагается на владельца TLS-сертификата.