

**Инструкция по переносу контейнера закрытого ключа на носители
(JaCarta LT и флеш-накопитель) и в реестр с использованием СКЗИ
КриптоПро CSP**

Листов 14

Оглавление

I. Введение	3
II. Добавление контейнеров закрытых ключей с CD диска	4
III. Добавление контейнеров закрытых ключей с флэш-накопителя	5
IV. Добавление сертификата в контейнер ключей КриптоПро CSP	7
V. Установка драйвера и перенос контейнера на JaCarta LT.....	10
VI. Перенос контейнера закрытого ключа с JaCarta LT в реестр.....	13

I. Введение

- ✓ Документ предназначен для пользователей, осуществляющих перенос контейнера закрытого ключа в реестр, на ключевой носитель JaCarta, либо на флэш-накопитель с использованием средства криптографической защиты информации (СКЗИ) КриптоПро CSP, а также установку сертификата в контейнер. Выберите необходимый раздел инструкции в зависимости от действия, которое хотите выполнить.
 - ✓ Данный документ предполагает, что перед переносом контейнеров закрытых ключей на Вашем автоматизированном рабочем месте (АРМ) уже установлено, зарегистрировано и настроено средство криптографической защиты информации (СКЗИ) КриптоПРО CSP.
 - ✓ **С 1 января 2022 года получить квалифицированный сертификат электронной подписи руководителя юридического лица или индивидуального предпринимателя можно только в государственных удостоверяющих центрах (ФНС, Федеральное казначейство, Центральный банк РФ)¹. В УЦ ИИТ можно получить сертификат на физическое лицо.**
 - ✓ Необходимо обращать особое внимание на примечания помеченные знаком .
-  **Всю необходимую документацию по услугам нашей компании вы можете загрузить на нашем сайте www.iitrust.ru раздел [«Поддержка»](#), кнопка [«Пользовательская документация»](#)**

¹ Согласно изменениям в 63-ФЗ «Об электронной подписи».

II. Добавление контейнеров закрытых ключей с CD диска

- ✓ В связи с особенностями программного комплекса Крипто Про CSP, при получении контейнеров закрытых ключей на CD диске, необходимо перенести ключевую информацию на флэш-накопитель, чтобы папка с ключами находилась в корневом каталоге (Рисунок 1).

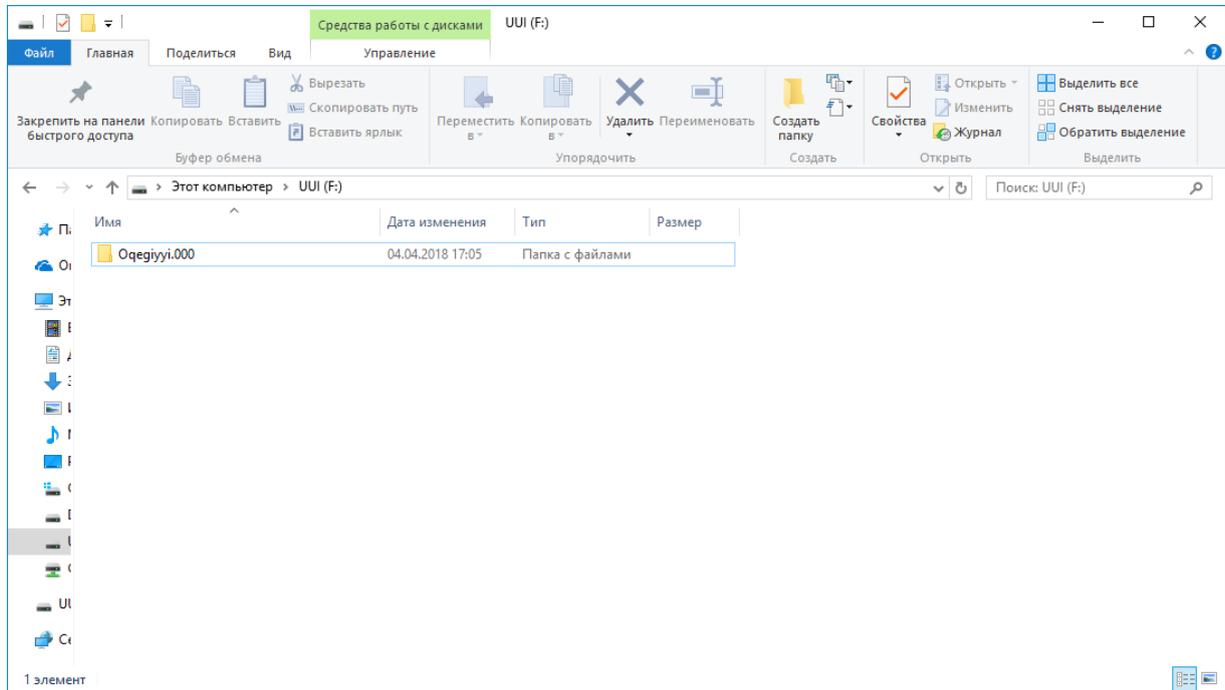


Рисунок 1

- ✓ Перейдите к III главе.

III. Добавление контейнеров закрытых ключей с флэш-накопителя

➔ **Внимание! Убедитесь, что флэш-накопитель находится в USB-порте Вашего компьютера**

1. Запустите КриптоПро CSP через меню «Пуск» → «Все программы» → «КРИПТО-ПРО» → «КриптоПро CSP», перейдите на вкладку «Оборудование» «Сервис» и нажмите кнопку «Скопировать...» (Рисунок 2).

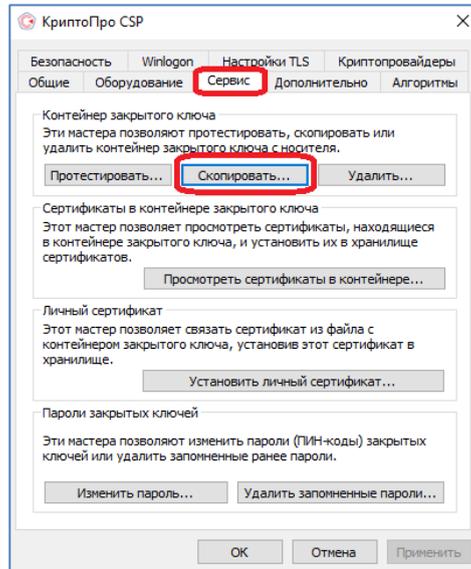


Рисунок 2

2. Нажмите кнопку «Обзор...» для выбора контейнера закрытого ключа, выберите нужный контейнер и нажмите кнопку «ОК» (Рисунок 3).

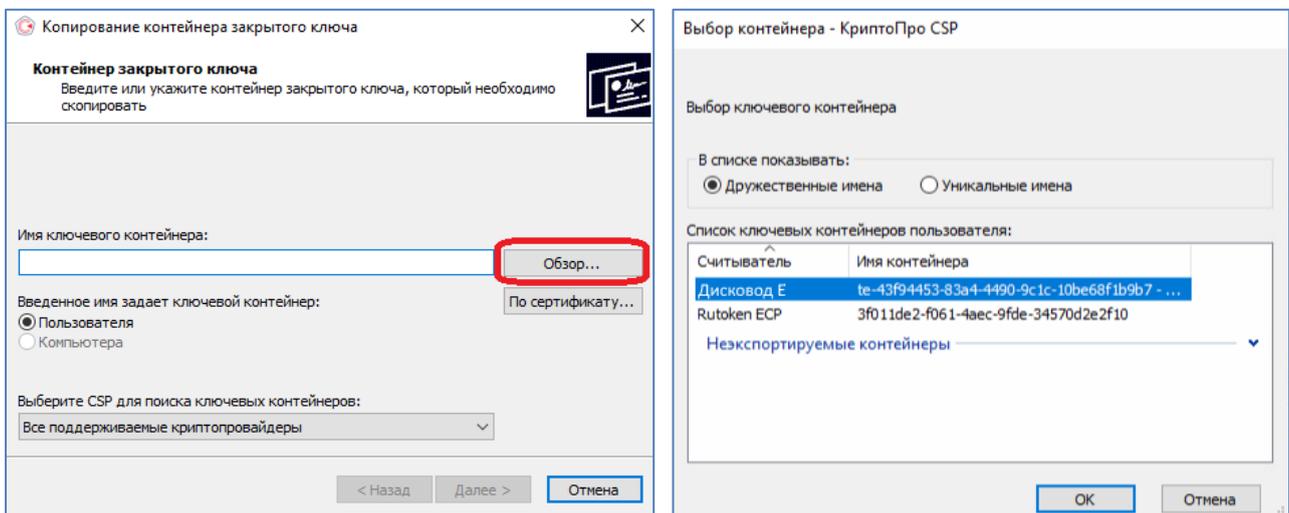


Рисунок 3

3. Задайте имя контейнера, который будет храниться в реестре, и нажать «Готово» (Рисунок 4).

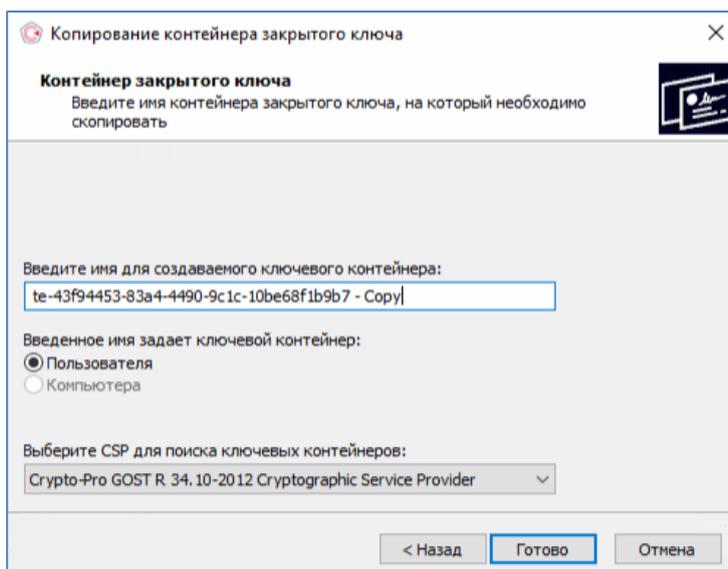


Рисунок 4

4. В окне выбора носителя необходимо выбрать **Реестр** и нажать **«OK»**, после чего ввести пароль. Если Вы хотите сохранить контейнер на ключевой носитель JaCarta LT, то в устройствах укажите **ARDS ZAO JaCarta LT 0**, при этом должно быть установлено ПО **«Единый клиент JaCarta»**, если его нет, перейдите к главе V² (Рисунок 5).

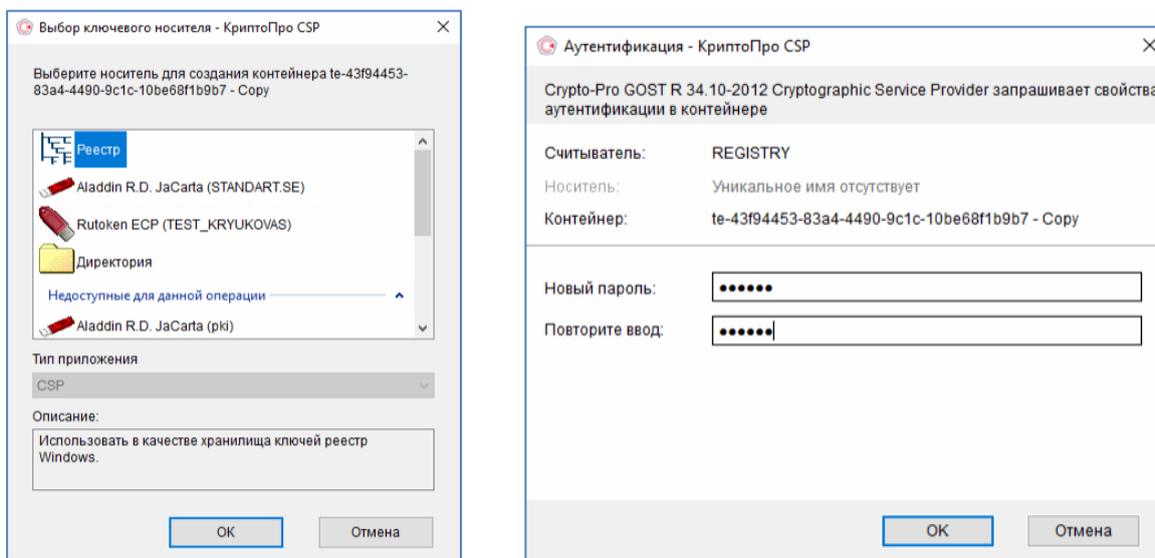


Рисунок 5

² По умолчанию PIN-код пользователя на устройство JaCarta LT:

- если носитель получен до 15.01.2019: **1eToken**
- с 15.01.19 года PIN -код устанавливается **1234567890**

IV. Добавление сертификата в контейнер ключей КриптоПро CSP

1. В основном окне КриптоПро CSP, перейдите на вкладку «*Сервис*» и нажмите кнопку «*Просмотреть сертификаты в контейнере*» (Рисунок 6).

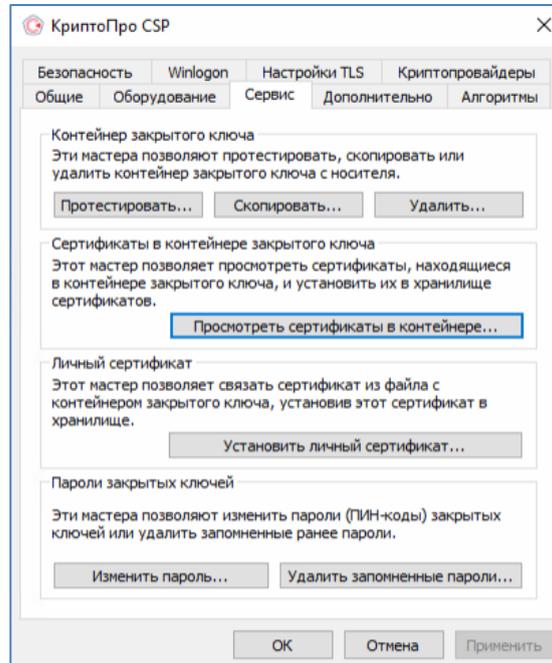


Рисунок 6

2. В открывшемся окне нажмите кнопку «*Обзор*», чтобы выбрать контейнер для просмотра.
 - Считыватель **ARDS ZAO JaCarta LT 0** – контейнер, сохранённый на JaCarta LT;
 - Считыватель **Диск [буква]** – контейнер, сохранённый на флеш карте;
 - Считыватель **Реестр** – контейнер, сохранённый на жестком диске ПК, в реестре.
 После выбора нужного контейнера нажмите кнопку «*Ок*» (Рисунок 7).

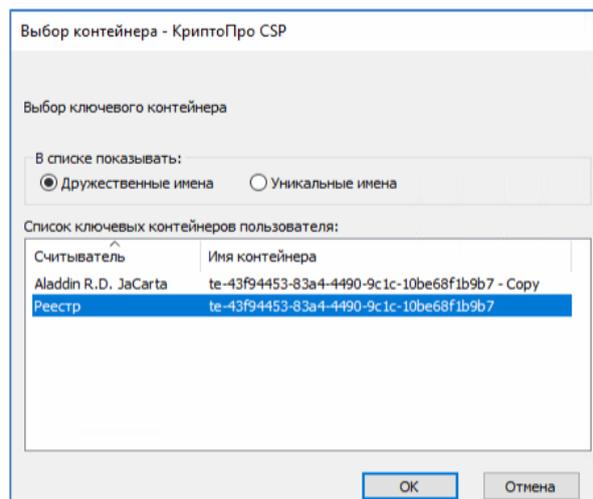


Рисунок 7

3. В следующем окне нажмите кнопку «*Далее*». Если запросит пароль, введите³.

³ По умолчанию PIN-код устройства JaCarta LT:

- если носитель получен до 15.01.2019: **1eToken**
- с 15.01.19 года PIN -код устанавливается **1234567890**

4. Далее в открывшемся окне нажмите на кнопку **«Установить»** (Рисунок 8). Если появится уведомление, что в контейнере закрытого ключа отсутствуют сертификаты, перейдите к пункту 7.

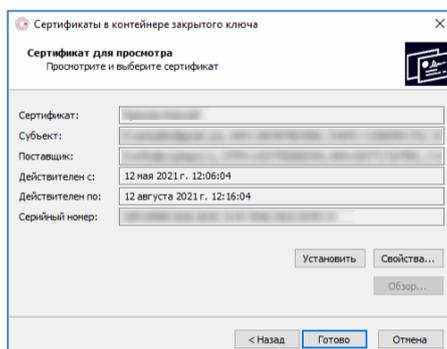


Рисунок 8

5. Если сертификат уже установлен в системном хранилище, появится уведомление о замене сертификата. Нажмите **«Да»** (Рисунок 9).

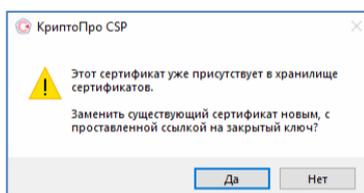


Рисунок 9

6. При появлении уведомления об отсутствии сертификатов в контейнер, нажмите на кнопку **«OK»** и перейдите к установке сертификата в контейнер (Рисунок 10).

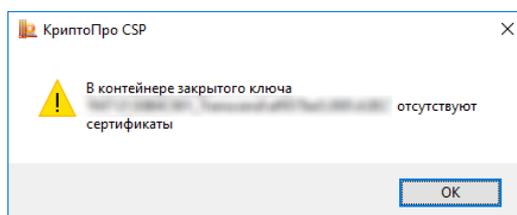


Рисунок 10

7. В окне **«Свойства КриптоПро CSP»** перейти на вкладку **«Сервис»** и нажмите на кнопку **«Установить личный сертификат»** (Рисунок 8).

8. В окне **«Мастер установки личного сертификата»** нажмите на кнопку **«Обзор»**, чтобы выбрать файл сертификата с расширением .cer, затем нажмите на кнопку **«Далее»** (Рисунок 11).

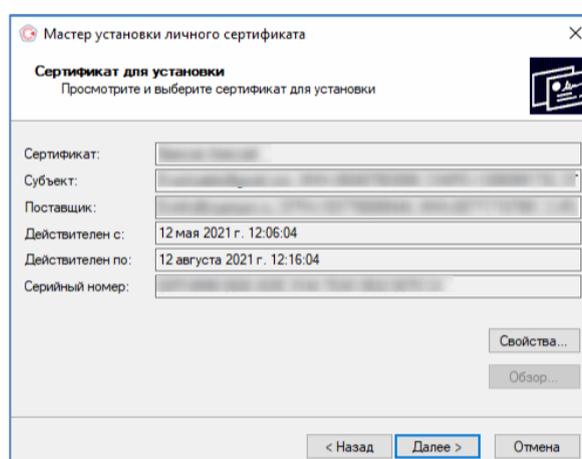
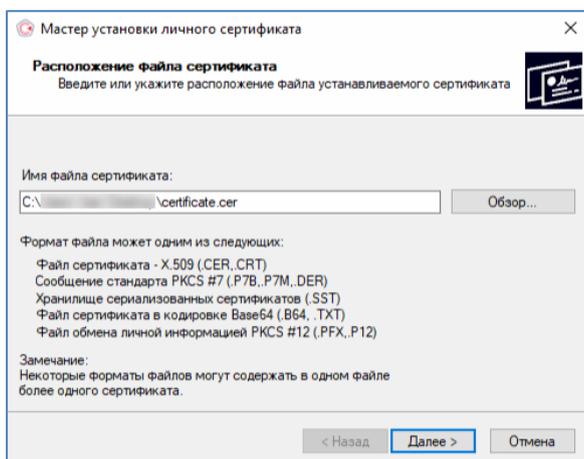


Рисунок 11

9. Установите галочку **«Найти контейнер автоматически»** - определится имя ключевого контейнера, нажмите на кнопку **«Далее»** (Рисунок 12).

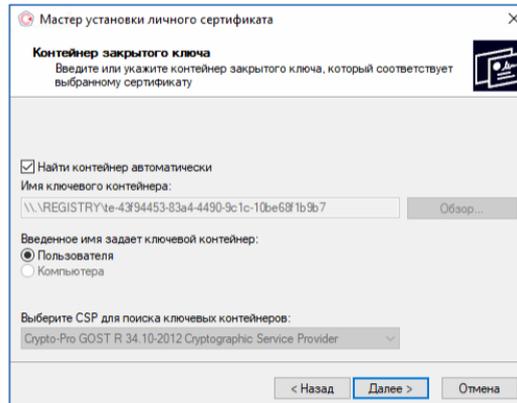


Рисунок 12

10. После выбора контейнера следует нажать на кнопку **«Далее»**. Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его. Введите пароль и нажмите кнопку **«Ок»**.

➔ По умолчанию ПИН-код на JaCarta LT: до 15.01.2019 устанавливался 1eToken, с 21.01.19 года устанавливается 1234567890, стандартный пароль к контейнеру, полученному на диске: 123456. Рекомендуется сменить ПИН доступа к JaCarta LT со стандартного на более устойчивый, который будете знать только Вы.

11. В окне **«Выбор хранилища сертификатов»** нажмите на кнопку **«Обзор»**. Необходимо выбрать хранилище **«Личные»** и нажать **«Ок»** (Рисунок 13).

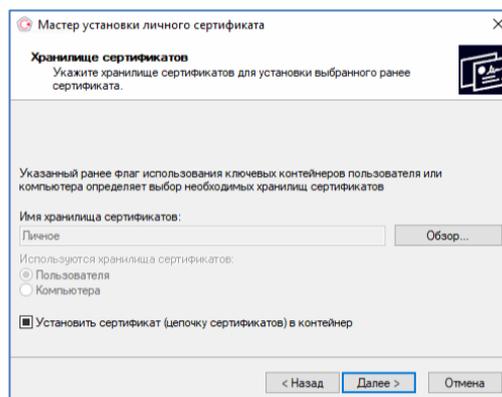


Рисунок 13

12. После выбора хранилища следует нажать на кнопку **«Далее»**, затем **«Готово»**. После нажатия на кнопку **«Готово»** может появиться сообщение (Рисунок 9). В таком случае необходимо выбрать **«Да»**. Дождаться сообщения об успешной установке.

V. Установка драйвера и перенос контейнера на JaCarta LT⁴

➔ **Внимание!** Данный пункт инструкции следует использовать, **ТОЛЬКО** если Вам выдали **ключевой носитель JaCarta LT**.

13. Для корректной работы ключевого носителя JaCarta LT под управлением операционной системы Microsoft Windows необходимо установить программное обеспечение, позволяющее выполнять базовые операции с электронными ключами JaCarta.

14. Для корректной работы ключевого носителя JaCarta LT под управлением операционной системы Microsoft Windows необходимо установить программное обеспечение, позволяющее выполнять базовые операции с электронными ключами JaCarta.

Для получения программного обеспечения актуальной версии необходимо зайти на страницу https://www.aladdin-rd.ru/support/downloads/jacarta_client, выбрать дистрибутив, подходящий разрядности вашей операционной системы, и нажать на кнопку «Скачать» (Рисунок 14).

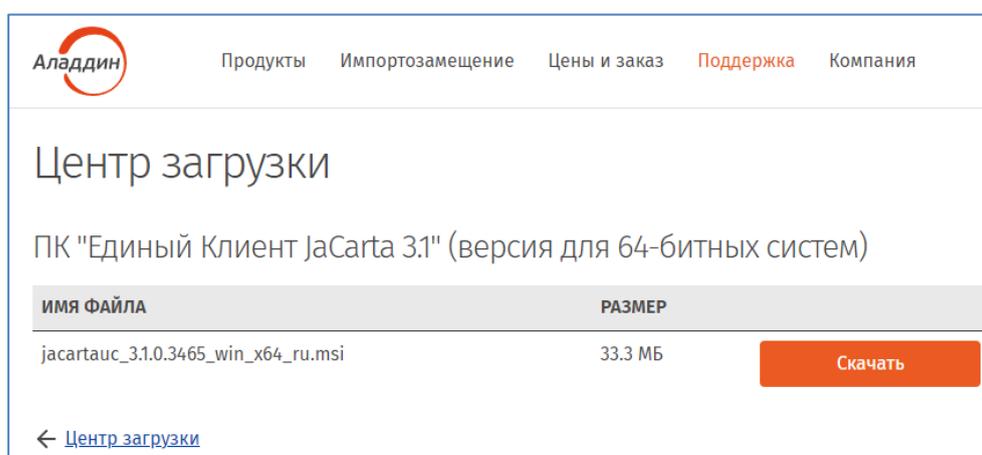


Рисунок 14

15. Загрузите дистрибутив в любое место компьютера и запустите установку утилиты. Выполните установку, следуя инструкциям мастера установки.

➔ **Внимание!** Убедитесь, что **ключевой носитель JaCarta LT находится в USB-порту Вашего компьютера**

4. Запустите криптопровайдер **КриптоПро CSP** из «Панели управления» или из кнопки меню «Пуск».

5. Перейдите на вкладку «Сервис» и нажмите кнопку «Скопировать...» (Рисунок 15).

⁴ Если вы используете ключевой носитель Rutoken, то вам необходимо установить программное обеспечение компании «Актив» по ссылке <https://www.rutoken.ru/support/download/windows/>.

Если вы используете ключевой носитель eToken, то вам необходимо установить программное обеспечение компании Алaddin РД «eToken PKI Client» по ссылкам:

- [для 64-разрядной системы;](#)

- [для 32-разрядной системы.](#)

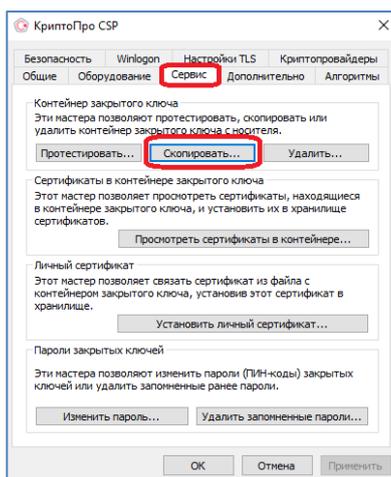


Рисунок 15

6. Нажмите кнопку **«Обзор...»** для выбора контейнера закрытого ключа, выберите нужный контейнер и нажмите кнопку **«OK»** (Рисунок 16).

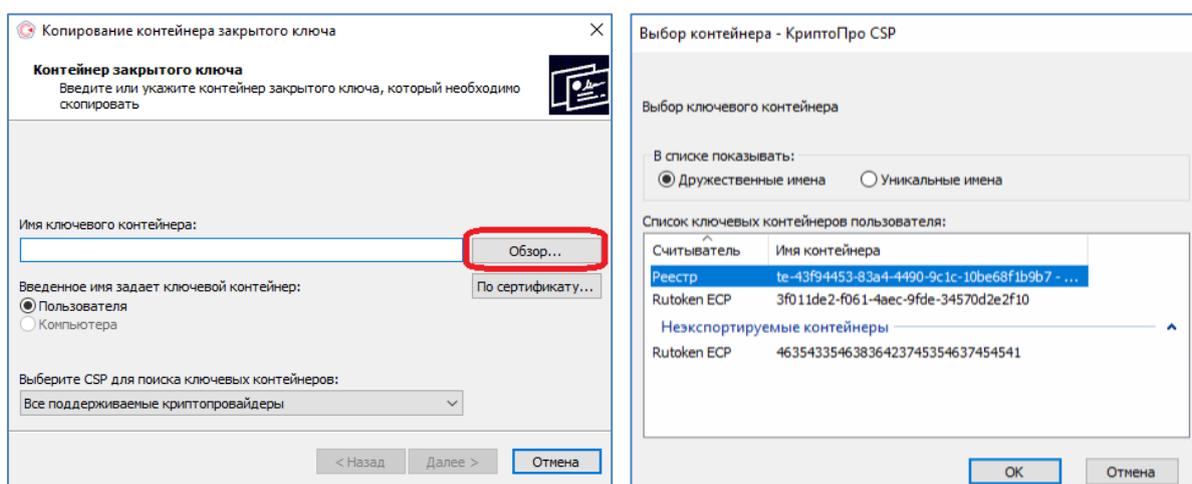


Рисунок 16

7. При необходимости введите пароль к контейнеру закрытого ключа ⁵ (Рисунок 17).

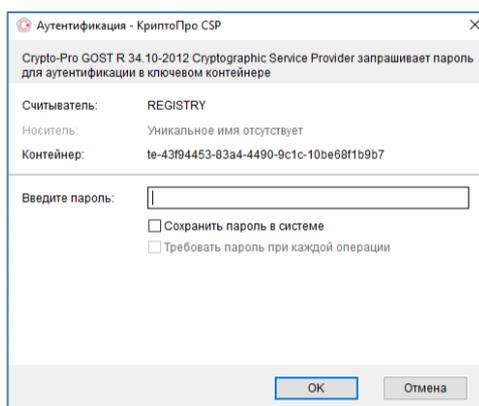


Рисунок 17

8. Задайте имя контейнера, который будет храниться на JaCarta LT, и нажмите **«Готово»** (Рисунок 18).

⁵ По умолчанию пин-код пользователя для контейнера: **123456**

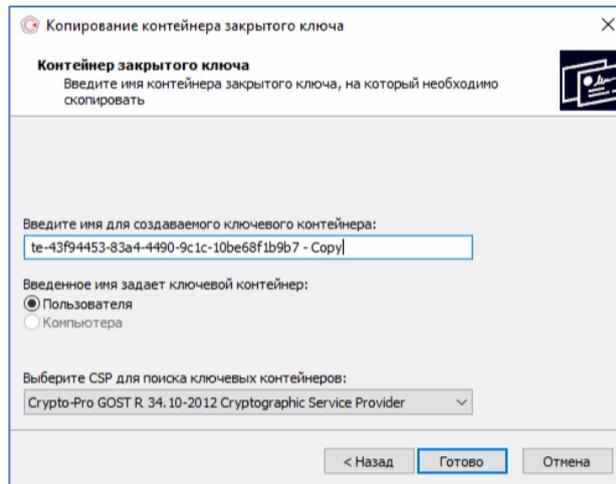


Рисунок 18

9. В окне выбора носителя укажите JaCarta LT **ARDS ZAO JaCarta LT 0** и нажмите **«OK»**, затем введите пароль для устройства JaCarta LT⁶ (Рисунок 19).

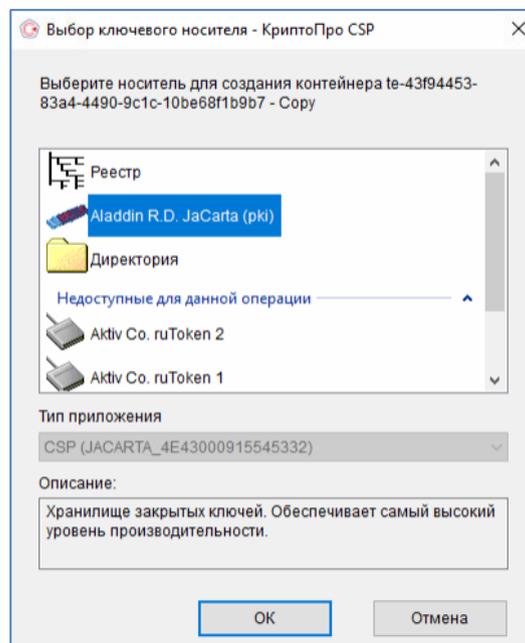


Рисунок 19

⁶ По умолчанию PIN-код пользователя на устройство JaCarta LT:

- если носитель получен до 15.01.2019: **1eToken**
- с 15.01.19 года PIN -код устанавливается **1234567890**

VI. Перенос контейнера закрытого ключа с JaCarta LT в реестр

➔ **Внимание! Убедитесь, что ключевой носитель JaCarta LT находится в USB-порте Вашего компьютера**

1. Запустите криптопровайдер **КриптоПро CSP** из «Панели управления» или из кнопки меню «Пуск».
2. Перейдите на вкладку «Сервис» и нажмите кнопку «Скопировать...» (Рисунок 20).

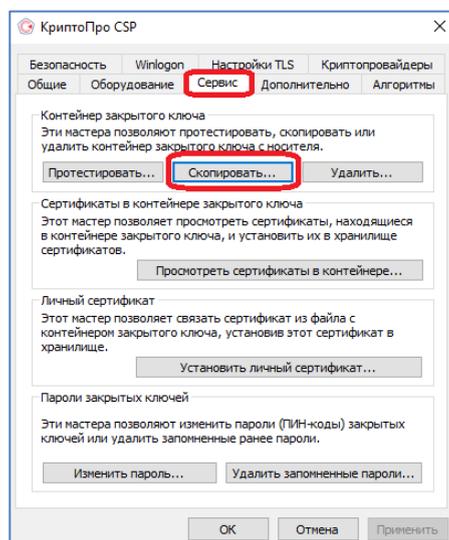


Рисунок 20

3. Нажмите кнопку «Обзор...» для выбора контейнера закрытого ключа, выберите нужный контейнер (Рисунок 21) и нажмите кнопку «ОК». Задайте имя контейнера, который будет храниться в реестре, и нажмите «Готово» (Рисунок 21).

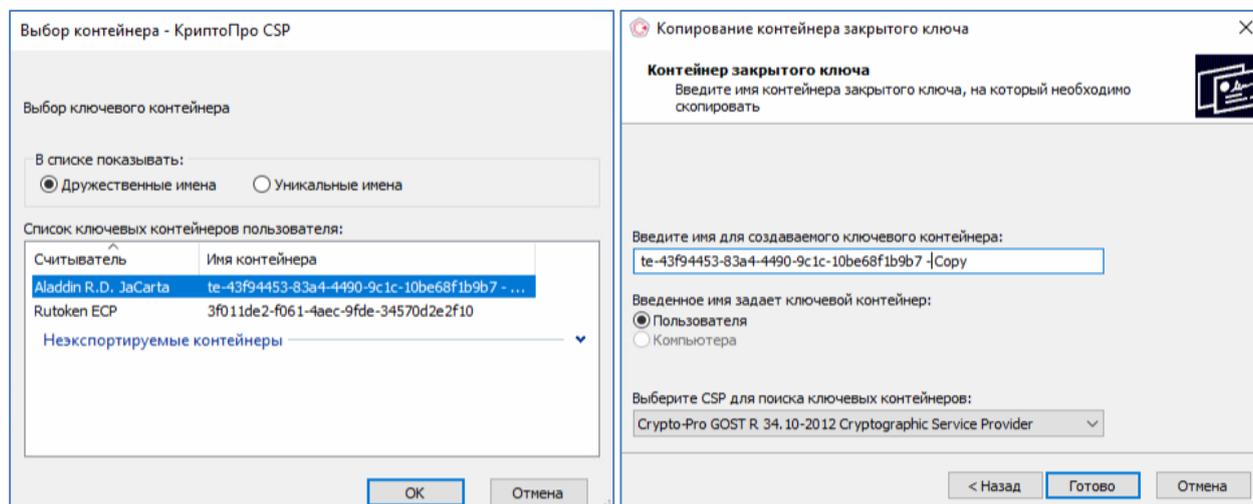


Рисунок 21

4. При необходимости введите пароль к носителю контейнера закрытых ключей JaCarta LT⁷.
5. В окне выбора ключевого носителя необходимо выбрать **Реестр** и нажать «Ок», после чего ввести пароль для контейнера ключей в реестре⁸ (Рисунок 22).

⁷ По умолчанию PIN-код пользователя на устройство JaCarta LT:

- если носитель получен до 15.01.2019: **1eToken**
- с 15.01.19 года PIN -код устанавливается **1234567890**

⁸ По умолчанию пин-код пользователя для контейнера: **123456**

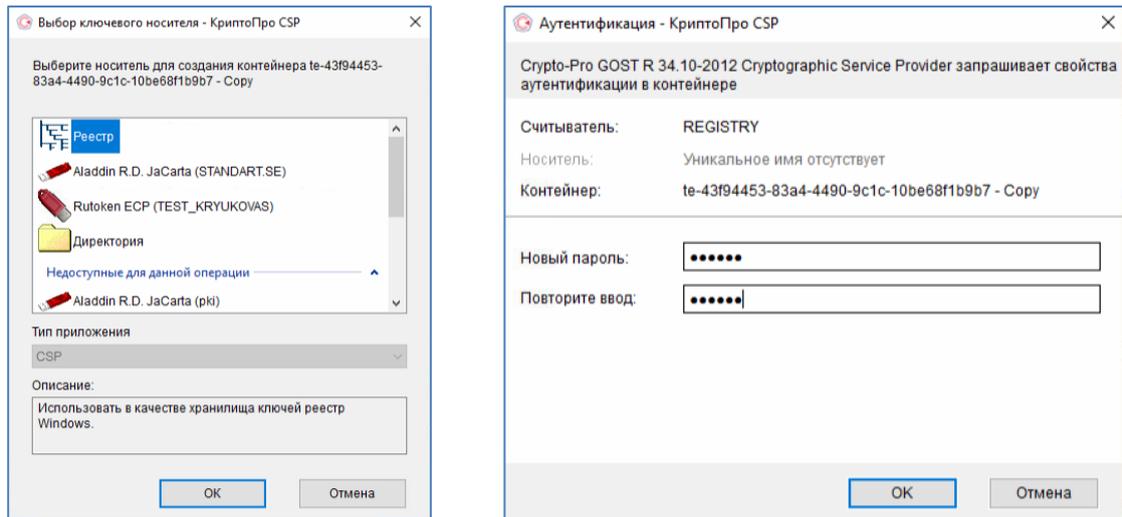


Рисунок 22