



uTrust

Руководство пользователя



ИНФОТЕКС
ТРАСТ

Содержание

Введение.....	3
Для кого предназначен документ.....	3
О программном обеспечении uTrust.....	3
Назначение программного обеспечения uTrust.....	3
Жизненный цикл запроса на сертификат.....	3
Системные требования	4
Обратная связь.....	4
Начало работы с программным обеспечением uTrust.....	5
Регистрация в программном обеспечении uTrust.....	5
Вход в программное обеспечение uTrust.....	5
Работа в программном обеспечении uTrust.....	7
Создание заявки на получение услуг удостоверяющего центра	7
Создание запроса на сертификат	15
Создание запроса на сертификат с помощью программы ViPNet CSP.....	15
Создание запроса на сертификат с помощью программы КриптоПро CSP	20
Установка сертификата	24
Глоссарий	26

Введение

Для кого предназначен документ

Данное руководство предназначено для пользователей программы для ЭВМ uTrust (далее – uTrust, личный кабинет, программное обеспечение), правообладателем которой является акционерное общество «Инфотекс Интернет Трест». В нем содержится подробная информация о функциональном назначении и возможностях использования программного обеспечения, а также о процедурах подачи заявок, генерации запроса на сертификат и установки сертификата на рабочее место.

О программном обеспечении uTrust

Назначение программного обеспечения uTrust

Программное обеспечение uTrust (далее - личный кабинет) — это ваш индивидуальный сервис с веб-интерфейсом для быстрого и удобного получения услуг удостоверяющего центра «Инфотекс Интернет Трест». Для получения сертификата ключа электронной подписи необходимо сначала создать заявку на получение услуг удостоверяющего центра (далее — УЦ), в которой передаётся информация о пользователе, а затем — создать запрос на сертификат.

Жизненный цикл запроса на сертификат

Основным сценарием работы с личным кабинетом является создание и обработка запроса на сертификат (рисунок 1).

Рисунок 1. Жизненный цикл запроса на сертификат

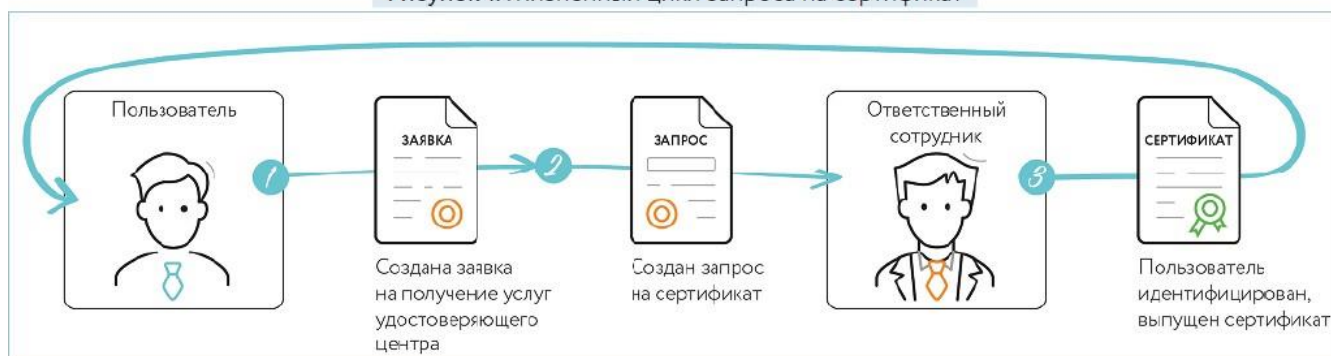


Рисунок 1. Жизненный цикл запроса на сертификат

Работа с запросом на сертификат происходит в следующем порядке:

- 1 Пользователь создаёт заявку на получение услуг удостоверяющего центра.
- 2 Пользователь в рамках этой заявки создаёт запрос на сертификат.
- 3 Ответственный сотрудник проводит идентификацию пользователя и издаёт сертификат.

Системные требования

Требования к компьютеру для работы с личным кабинетом:

- браузеры:
 - Internet Explorer 10 или более поздней версии;
 - Google Chrome актуальной версии;
 - Mozilla Firefox актуальной версии.
- криптопровайдеры:
 - ViPNet CSP последней доступной версии;
 - КриптоПро CSP последней доступной версии;
 - JCrypto последней доступной версии;
 - криптопровайдеры, встроенные в токен.
- дополнительное программное обеспечение:
 - JavaLSS;
 - JC-WebClient.

Обратная связь

Для решения возникающих проблем обратитесь в службу технической поддержки компании «Инфотекс Интернет Траст»:

- электронный адрес службы поддержки: supportIT@iitrust.ru;
- форма запроса в службу технической поддержки: <http://www.iitrust.ru/support/request.php>;
- 8 (800) 250-0-265 — «горячая линия» службы технической поддержки (звонок бесплатный для любого региона);
- 8 (800) 250-8-265 — «горячая линия» службы продаж и абонентского обслуживания (звонок бесплатный для любого региона).

Начало работы с программным обеспечением uTrust

Регистрация в программном обеспечении uTrust

Для начала работы с uTrust вам не нужно проходить отдельную процедуру регистрации. Если вас ещё нет учётной записи для входа в uTrust, то она будет создана автоматически в процессе создания заявки на получение услуг УЦ (см. [Создание заявки на получение услуг удостоверяющего центра](#)).

Вход в программное обеспечение uTrust

Чтобы просмотреть свои заявки и создать запрос на сертификат (см. [Создание запроса на сертификат](#)), предварительно войдите в личный кабинет. Для этого выполните следующие действия:

- 1 Откройте веб-сайт личного кабинета. Для этого перейдите по ссылке, полученной у вашего персонального менеджера (см. [гlossарий](#)).
- 2 Нажмите «Войти». Откроется страница входа.



8 800 250-8-265 8 800 250-0-265
Звонок бесплатный Техподдержка 24/7

ВОЙТИ



ИнфоТеКС Интернет Траст —

российский оператор электронного документооборота.

Мы обеспечиваем безопасный обмен данными, автоматизируем бухгалтер и выпускаем квалифицированную электронную подпись.



Рисунок 2. Просмотр страницы входа в личный кабинет

- 3 В соответствующих полях введите логин и пароль от личного кабинета. Если вы ещё не зарегистрированы, выберите услугу, подайте заявку и вам автоматически будет создан ваш личный кабинет.
- 4 Нажмите кнопку «Войти» (рисунок 3).

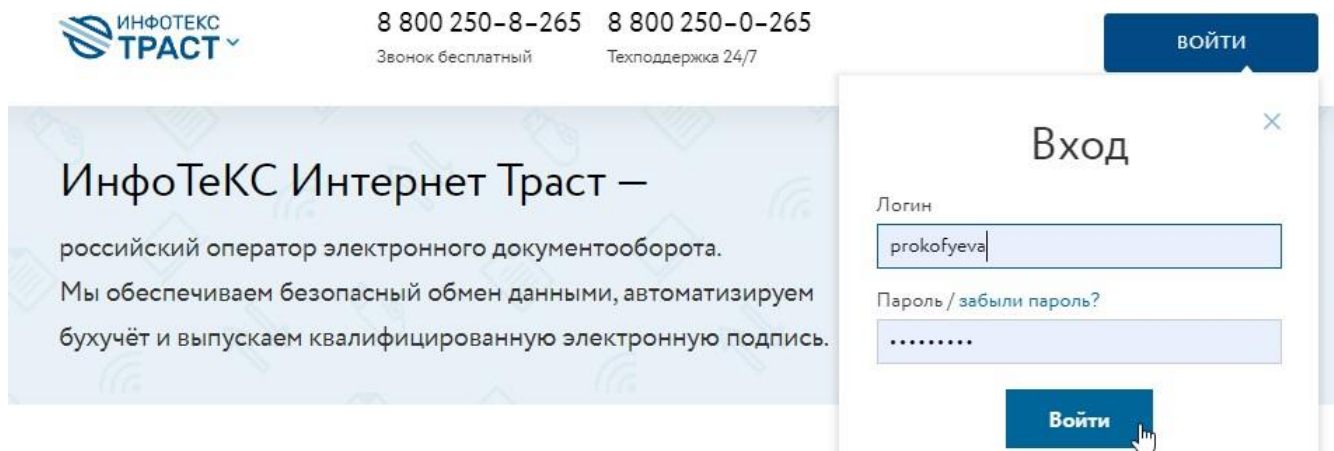


Рисунок 3. Ввод учётных данных пользователя для входа в личный кабинет

Работа в программном обеспечении uTrust

Создание заявки на получение услуг удостоверяющего центра

Для получения сертификата ключа электронной подписи необходимо сначала создать заявку на получение услуг удостоверяющего центра (далее — УЦ), в которой передаётся информация о пользователе, а затем — создать запрос на сертификат. Заявка может быть сформирована лично пользователем, или вместо него сформировать заявку на получение услуг УЦ может ответственный сотрудник. Сгенерировать запрос на сертификат может только пользователь.

В заявке указывается регистрационная информация пользователя:

- фамилия, имя и отчество (если имеется);
- наименование должности;
- наименование организации;
- СНИЛС;
- реквизиты паспорта гражданина РФ.

Чтобы создать заявку на получение услуг удостоверяющего центра, выполните следующие действия:

- 1** Если у вас уже есть учётная запись, войдите в нее. Если учётной записи у вас нет, перейдите по ссылке, полученной у представителя удостоверяющего центра.
- 2** На главной странице личного кабинета в разделе «Заказать электронную подпись» выберите тип заявки на получение услуг удостоверяющего центра (рисунок 4).

ИнфоТеКС Интернет Траст —

российский оператор электронного документооборота.

Мы обеспечиваем безопасный обмен данными, автоматизируем бухгалтер и выпускаем квалифицированную электронную подпись.



Заказать электронную подпись

Выберите один из популярных сертификатов электронной подписи

Базовый сертификат

Конструктор сертификата. Позволяет получить базовый сертификат, который расширяется федеральными и коммерческими электронными торговыми площадками, порталом Росреестра и другими государственными информационными системами.

от 1 500 ₽

Специализированный квалифицированный сертификат ЕГАИС ФСРАР РФ

Сертификат для Единой государственной автоматизированной системы Федеральной службы по регулированию алкогольного рынка РФ.

Специализированный квалифицированный сертификат ЕГАИС ФСРАР РФ (ПРОДЛЕНИЕ)

Продление сертификата для Единой государственной автоматизированной системы Федеральной службы по регулированию алкогольного рынка РФ.

Рисунок 4. Выбор типа сертификата в разделе «Заказать электронную подпись»

- 3 На странице «Сертификат» выберите тип заявителя и необходимые расширения. Нажмите кнопку «Продолжить» (рисунок 5).

Сертификат

Точка выдачи

Реквизиты

Личные данные

Оплата

Заявитель

☒ Юридическое лицо
 ☐ Индивидуальный предприниматель
 ☐ Физическое лицо

Расширения

Базовый сертификат

☒ Базовый сертификат

Электронные торговые площадки

☐ Федеральные ЭТП – РТС-тендер, Сбербанк-АСТ, ЕЭТП, Национальная электронная площадка, zakazrf.ru, АСТ ГОЗ (Участник размещения заказа), ЭТП РАД
 ☐ Ассоциация ЭТП (включая uTender)
 ☐ Центр дистанционных торгов - Участник торгов (покупатель)
 ☐ Центр электронных торгов B2B (b2b-center.ru)
 ☐ Сибирская торговая площадка
 ☐ Электронная торговая площадка ГПБ (etp.gpb.ru)
 ☐ Центр реализации
 ☐ ЭТП Арбитрат
 ☐ ЭТП ТЭК-Torg
 ☐ ЭТП Tender.one
 ☐ ЭТП UralBidIn
 ☐ Региональная торговая площадка (regtorg.com)
 ☐ Электронные системы Поволжья
 ☐ Уральская ЭТП
 ☐ Торговый портал Фабрикант
 ☐ ЭТП Фритрейд
 ☐ ЭТП Alfalot.ru
 ☐ ЭТП Аукционный тендерный центр
 ☐ Агентство экономической информации ПРАЙМ
 ☐ СКРИН
 ☐ АЗИПИ (Ассоциация защиты информационных прав инвесторов)
 ☐ Система раскрытия информации АК&М
 ☐ Портал Росреестра
 ☐ Расширение ФРДО

Внимание! При работе в ФИС ФРДО используется ПО ViPNet Client, которое в своем составе имеет СКЗИ ViPNet CSP. Во избежании конфликта криптопровайдеров, рекомендуем формировать запрос на подпись под СКЗИ ViPNet CSP.

Дополнительные услуги

☐ USB-токен JaCarta LT
 ☐ Срочный выпуск сертификата

Выпуск сертификата в течение часа, стандартный срок – 2-3 рабочих дня. Перед посещением точки выдачи загрузите платежное поручение в Личный кабинет.

☐ Настройка рабочего места, консультация по работе с сертификатом

Специалисты работают по будням с 09:00 до 18:00 (по Мск). Требуется предварительная запись.

Заполнено:

1 из 5

Ваш заказ

Базовый сертификат

Всего

1 900 Р

Продолжить

Рисунок 5. Выбор сфер применения сертификата

uTrust (ЛК пользователя УЦ). Руководство Пользователя 9

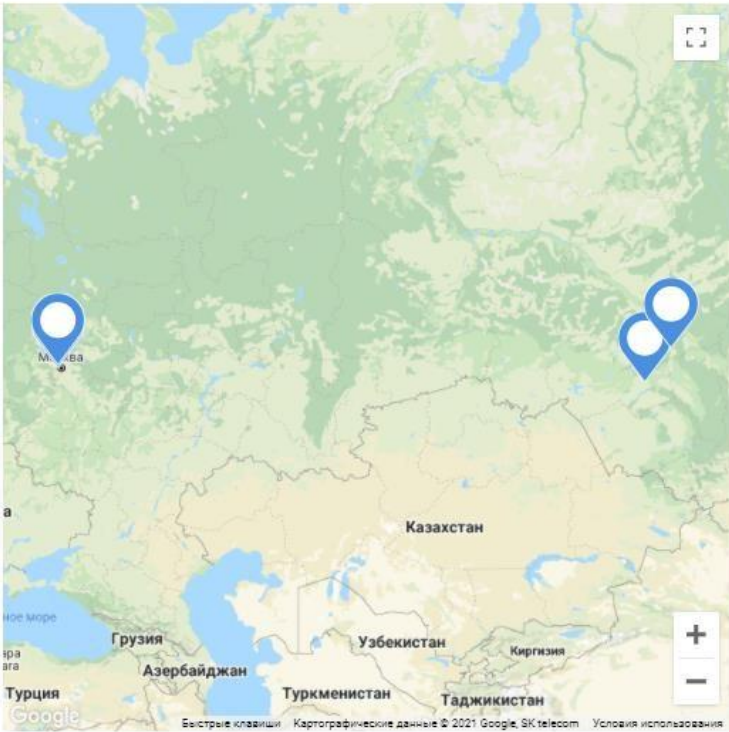
- 4 На странице «Точка выдачи» просмотрите адрес точки выдачи сертификата (адрес расположения ответственного сотрудника) и нажмите кнопку «Продолжить» (рисунок 6).

Базовый сертификат

Сертификат **Точка выдачи** Реквизиты Личные данные Оплата

Регион
г. Москва

Поиск



☐ Тестовый ЛК
г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1

☐ Тестовая точка выдачи
г. Москва, Петровско-Разумовский пр-д, 1/23, строение 1

☐ для Антонова
г. Москва

☐ для Чернова
г. Москва

☐ для Данилова
г. Москва, Старый Петровско-Разумовский проезд, д. 1/23с.1
Пн-пт, 09:00 – 18:00. Без перерыва. Сб, вс - выходной

☐ Точка выдачи для И. Петраковой
г. Москва

☐ Точка выдачи ЕСРП
г. Москва

☐ Точка выдачи для К. Боровского
г. Москва

☐ Точка выдачи коммерческого департамента
г. Москва

☐ Срочный выпуск
г. Москва, Первый проезд, 15
Пн-пт, 09:00 – 18:00. Без перерыва. Сб, вс - выходной

← Назад

Продолжить

Рисунок 6. Выбор точки выдачи сертификата

- 5 В случае, если заявитель – ЮЛ, на странице «Реквизиты» укажите ИНН (рисунок 7).

Базовый сертификат

Сертификат Точка выдачи **Реквизиты** Личные данные Оплата

ИНН

Узнать и проверить ИНН

Заполнено:
3 из 5

Заявитель
Юридическое лицо

Точка выдачи
для Прокофьевой
г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2,
пом. IX, ком. 11
olesya.prokofyeva@iitrust.ru

Ваш заказ
Базовый сертификат

Всего

1 900 ₽

Рисунок 7. Ввод ИНН

Реквизиты организации загружаются автоматически по ИНН вашей организации. В соответствующих полях проверьте и отредактируйте реквизиты вашей организации и нажмите кнопку «Продолжить» (рисунок 8).

Базовый сертификат

СертификатТочка выдачиРеквизитыЛичные данныеОплата

ИНН

7743020560

У обособленных подразделений один ИНН, а название, КПП и адрес — разные.

Организация

АО "ИИТ"

КПП

771401001

Юридический адрес

Регион

город Москва

Город

город Москва

Улица

улица Мишина

☐ Отсутствует

Корпус/Дом

Д 56, СТР 2

☐ Отсутствует

Офис/кв.

ЭТАЖ, ПОМЕЩ, КОМ 2/IX/11

Заполнено:
3 из 5

Заявитель

Юридическое лицо

Точка выдачи

для Прокофьевой
г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2,
пом. IX, кон. 11
olesya.prokofyeva@iitrust.ru

Ваш заказ

Базовый сертификат

Всего

1900 Р

[← Назад](#)

Продолжить

Внимательно проверьте данные.
Они — часть сертификата.

Рисунок 8. Редактирование реквизитов организации.

- 6 На странице «Личные данные» в разделе «Данные владельца сертификата» укажите личные данные пользователя (рисунок 9).

Сертификат

Точка выдачи

Реквизиты

Личные данные

Оплата

Данные владельца сертификата

Фамилия

Прокофьева

Имя

Олеся

Отчество

Алексеевна

✕

Отчество отсутствует

СНИЛС

ИНН

771821550426

Если вы не знаете свой ИНН, то можете его найти на сайте ФНС.

Мобильный телефон

+7 999 999-99-99

Электронная почта

fhudshsur@ya.ru

На электронную почту придет логин и пароль от личного кабинета. Если в сертификат нужно добавить другой адрес, укажите его в поле ниже.

Добавить электронную почту для сертификата

Адрес

Регион



Московская область

Город

город Реутов

Добавить контактное лицо

Заполнено:
4 из 5



Заявитель

Физическое лицо

Точка выдачи

для Прокофьевой
г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2,
пом. IX, ком. 11
olesya.prokofyeva@iitrust.ru

Ваш заказ

Базовый сертификат
Портал Росреестра

Всего

2 500 Р

← Назад

Продолжить

Отправляя заявку, я соглашаюсь с Политикой обработки персональных данных АО «ИИТ».

Рисунок 9. Указание данных о пользователе


uTrust (ЛК пользователя УЦ). Руководство Пользователя 13

- 7 На странице «Оплата» выберите форму оплаты. Для ФЛ/ИП — по карте или счёту, для ЮЛ — только по счёту (рисунок 10).

Базовый сертификат

Сертификат Точка выдачи Реквизиты Личные данные **Оплата**

Форма оплаты

☐ Оплата картой 
Оплата картами недоступна для юридических лиц.

☒ **Оплата по счёту**

Заполнено: **5 из 5**

Заявитель
Юридическое лицо

Точка выдачи
для Прокофьевой
г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2,
пом. IX, ком. 11
olesya.prokofyeva@iitrust.ru

Ваш заказ
Базовый сертификат

Всего 1 900 ₽

← Назад **Оформить заявку**

Рисунок 10. Выбор формы оплаты

Появится сообщение о том, что заявка успешно оформлена. После создания заявки вы получите по электронной почте письмо с вашими учётными данными для входа в личный кабинет (если вы создавали заявку впервые). Войдите в личный кабинет и создайте запрос на сертификат (см. [Создание запроса на сертификат](#)).

Создание запроса на сертификат

После того, как Вы создали заявку на получение услуг удостоверяющего центра, вы можете создать запрос на сертификат. В зависимости от установленного на вашем компьютере криптопровайдера следуйте указаниям одного из разделов:

- [Создание запроса на сертификат с помощью программы ViPNet CSP](#)
- [Создание запроса на сертификат с помощью программы КриптоПро CSP](#)

Внимание! Генерировать запрос можно:

1. На компьютер, на котором будет происходить дальнейшая работа с сертификатом.
2. На токен (при использовании токена не забудьте подключить его к компьютеру).

Создание запроса на сертификата с помощью программы ViPNet CSP

Чтобы создать запрос на сертификат с помощью программы ViPNet CSP, выполните следующие действия:

- 1 Войдите в Личный кабинет (см. [Вход в программное обеспечение uTrust](#)).
- 2 После входа в личный кабинет вы увидите список ваших заявок. Щёлкните номер заявки в статусе «Ожидание запроса на сертификат» (рисунок 11).

Номер	Клиент	Дата подачи	Точка выдачи	Стоимость	Статус	Сертификат
4296	АО "ИИИТ": Пркоофьева Олеся Алексеевна	12.10.2021	77 - для Прокофьевой	1900 Оплачено	Ожидание запроса на сертификат	

Рисунок 11. Просмотр списка заявок

- 3 Откроется страница просмотра заявки. если на панель «Процесс» вы видите сообщение о необходимости установки дополнительного программного обеспечения, выполните его установку, перейдя по ссылке (рисунок 12).



Рисунок 12. Просмотр сообщения о необходимости установки дополнительного программного обеспечения

- 4 На панели «Процесс» нажмите кнопку «Сгенерировать запрос» (рисунок 13).

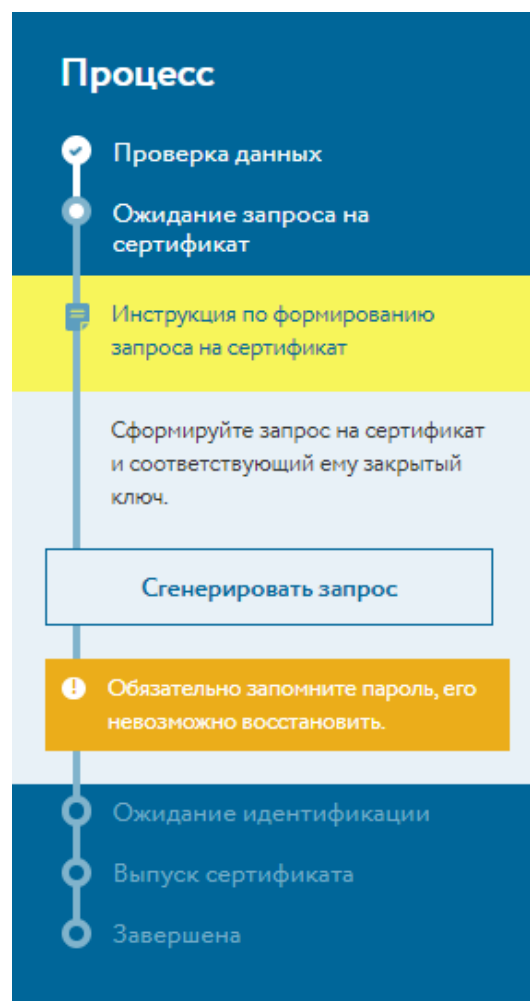


Рисунок 13. Создание запроса на сертификат



Внимание! Далее в этом разделе описано создание контейнера ключей в программе ViPNet CSP. Если вы используете другой криптопровайдер, следуйте подготовленной для него инструкции.

- 5 В окне «Создание ключа электронной подписи» в списке «Использовать криптопровайдер» выберите Infotecs Cryptographic Service Provider и нажмите кнопку «Создать ключ электронной подписи» (рисунок 14).

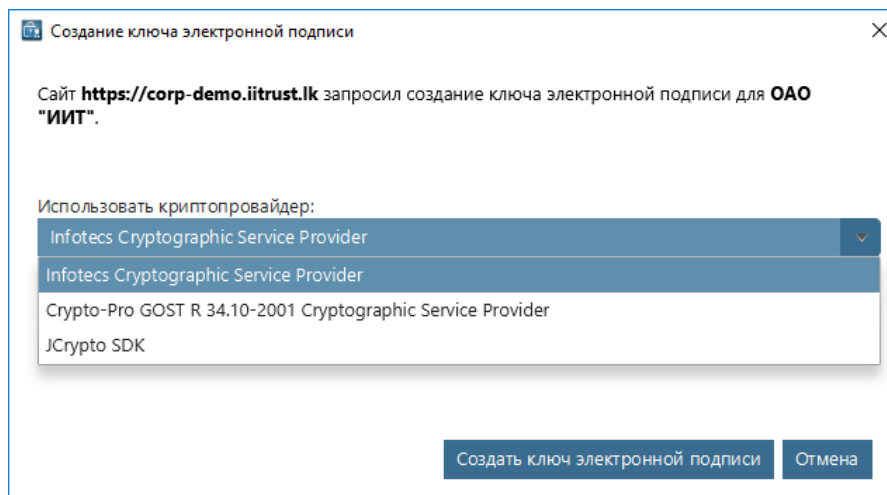


Рисунок 14. Выбор криптопровайдера

- 6 В появившемся окне «ViPNet CSP — инициализация контейнера ключей» укажите следующее:
- имя контейнера ключей (или оставьте значение по умолчанию в соответствующем поле);
 - место размещения контейнера ключей, установив переключатель в одно из значений: «Папка на диске» или «Выберите устройство».
- В зависимости от места размещения контейнера ключей в запрос будет добавлено расширение со следующей информацией:
- при размещении контейнера ключей в папке на диске — с информацией о том, что желаемый срок действия закрытого ключа — 1 год;
 - при размещении контейнера ключей на устройстве с аппаратной поддержкой алгоритмов ГОСТ — с информацией о том, что желаемый срок действия закрытого ключа — 3 года.

Нажмите кнопку ОК (рисунок 15).

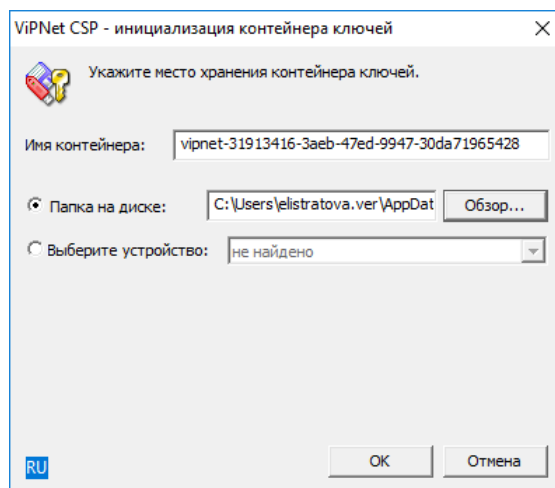


Рисунок 15. Выбор места хранения контейнера ключей.

- 7 В окне ViPNet CSP — пароль контейнера ключей задайте пароль доступа к контейнеру ключей.



Внимание! Обязательно запомните пароль, восстановить его нельзя. Если вы потеряете пароль, необходимо будет создавать новую заявку.

Установите флажок «Сохранить пароль», если не хотите в дальнейшем вводить пароль к этому контейнеру ключей и нажмите кнопку ОК (рисунок 16).

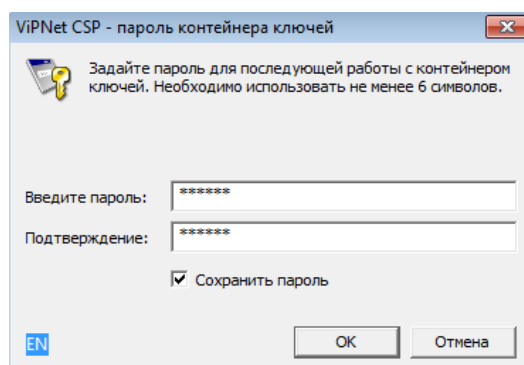


Рисунок 16. Создание пароля контейнера ключей

- 8 Появится электронная рулетка. Поводите указателем в пределах окна «Электронная рулетка» (рисунок 17).

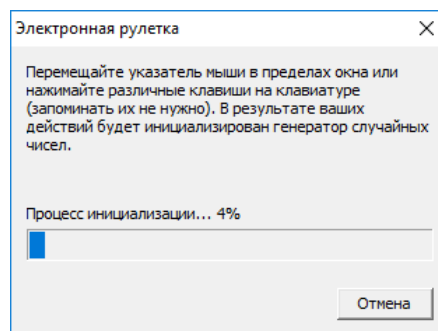


Рисунок 17. Просмотр окна «Электронная рулетка»

- 9 Если при создании пароля доступа к контейнеру ключей вы не установили флажок «Сохранить пароль», в следующем окне введите пароль. Нажмите кнопку ОК.

- 10 Ваша заявка получит статус «Ожидание идентификации» (рисунок 18).

Реквизиты

Документы

Владелец

ФИО Прокофьева Олеся Алексеевна

СНИЛС

ИНН ФЛ

Должность Тест

Почта hydtyuy@ya.ru

Почта в сертификат hydtyuy@ya.ru

Телефон +7 999 999-99-99

Реквизиты

Роль Юридическое лицо

Наименование АО "ИИТ"

ИНН 7743020560

КПП 771401001

ОГРН 1027739113049

Адрес г. Москва, г. Москва, ул. Мишина, д. 56, СТР 2, ЭТАЖ, ПОМЕЩ, КОМ 2/IX/11

Процесс

- ✓ Проверка данных
- ✓ Ожидание оплаты
- ✓ Ожидание запроса на сертификат
- Ожидание идентификации

Для получения сертификата обратитесь в точку выдачи.

Подробная информация отправлена на электронную почту hydtyuy@ya.ru.

- Выпуск сертификата
- Формирование отгрузочных документов
- Ожидание подтверждения завершения
- Завершена

Рисунок 18. Ожидание идентификации

Для прохождения идентификации и получения сертификата обратитесь в точку выдачи, которую вы выбрали ранее. Для прохождения идентификации вам понадобится предоставить сотруднику необходимые документы, а также расписаться в предоставленном сотрудником бланке сертификата. Как только вы пройдёте идентификацию у ответственного сотрудника, сертификат будет издан, и вы сможете установить его.

Создание запроса на сертификат с помощью программы КриптоПро CSP

Чтобы создать запрос на сертификат с помощью программы КриптоПро CSP, выполните следующие действия:

- 1 Войдите в личный кабинет (см. [Вход в программное обеспечение uTrust](#)).
- 2 После входа в личный кабинет вы увидите список ваших заявок. Щёлкните номер заявки в статусе «Ожидание запроса на сертификат» (рисунок 19).

Номер	Клиент	Дата подачи	Точка выдачи	Стоимость	Статус	Сертификат
4296	АО "ИИИТ": Пркоофьева Олеся Алексеевна	12.10.2021	77 - для Прокофьевой	1900 Оплачено	Ожидание запроса на сертификат	

Рисунок 19. Просмотр списка заявок

- 3 Откроется страница просмотра заявки. Если на панели «Процесс» вы видите сообщение о необходимости установки дополнительного программного обеспечения, выполните его установку (рисунок 20).



Рисунок 20. Просмотр сообщения о необходимости установки дополнительного программного обеспечения

- 4 На панели «Процесс» нажмите кнопку «Сгенерировать запрос» (рисунок 21).

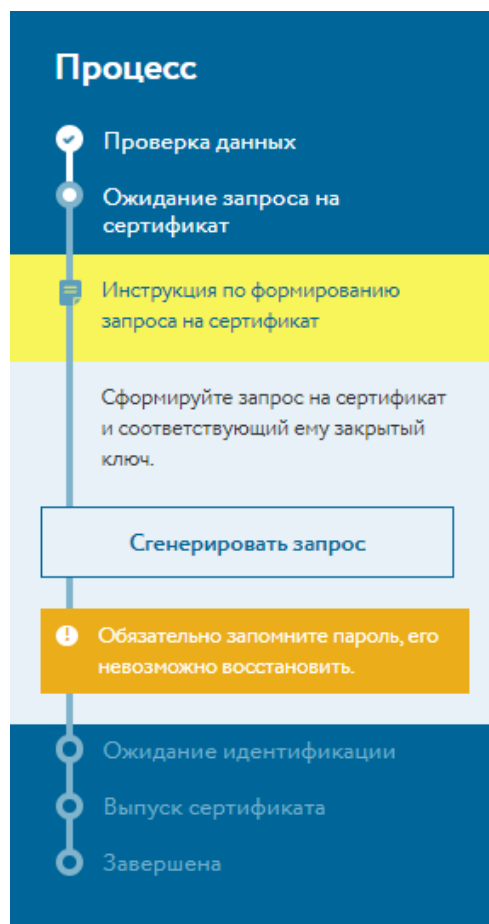


Рисунок 21. Создание запроса на сертификат



Внимание! Далее в этом разделе описано создание контейнера ключей в программе КриптоПро CSP. Если вы используете другой криптопровайдер, следуйте подготовленной для него инструкции.

- 5 В окне «Создание ключа электронной подписи» в списке «Использовать криптопровайдер» выберите Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider и нажмите кнопку «Создать ключ электронной подписи» (рисунок 22).

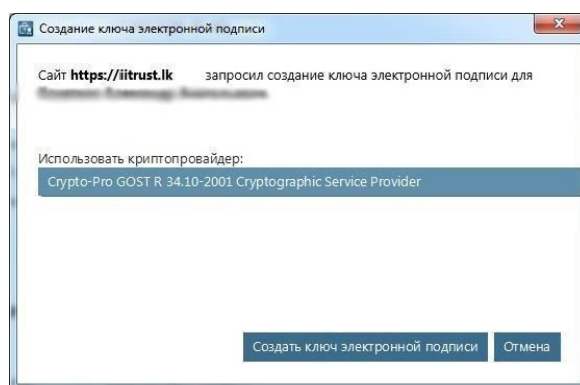


Рисунок 22. Выбор криптопровайдера для создания ключа электронной подписи

- 6 В появившемся окне КриптоПро CSP выберите носитель для хранения контейнера ключей и нажмите кнопку «ОК» (рисунок 23).

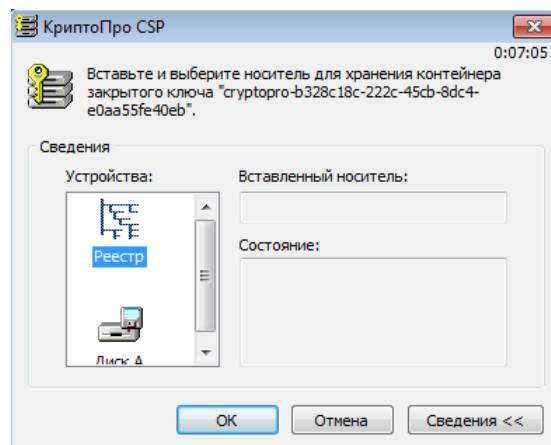


Рисунок 23. Выбор места хранения контейнера ключей

- 7 Появится электронная рулетка. Поводите указателем в пределах окна электронной рулетки (рисунок 24).

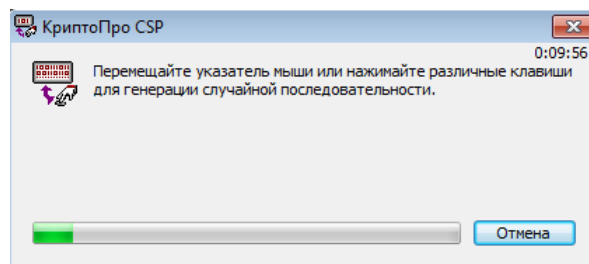


Рисунок 24. Просмотр окна «Электронная рулетка»

- 8 В окне КриптоПро CSP задайте пароль доступа к контейнеру ключей и подтвердите его. Нажмите кнопку «ОК» (рисунок 25).

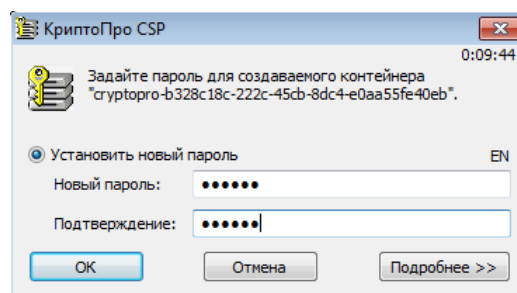


Рисунок 25. Установка пароля доступа к контейнеру ключей

- 9 Введите пароль доступа к контейнеру ключей. Установите флажок «Запомнить пароль», если не хотите в дальнейшем вводить пароль к этому контейнеру ключей. Нажмите кнопку «ОК» (рисунок 26).

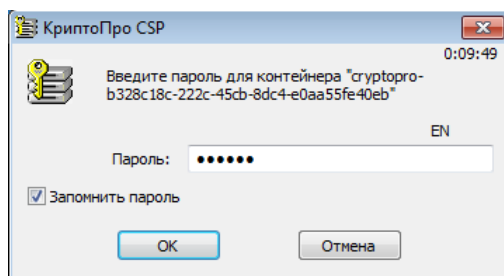


Рисунок 26. Ввод пароля для контейнера ключей

10 Ваша заявка получит статус «Ожидание идентификации» (рисунок 27).

Заявка №4296

Базовый сертификат

Ожидание идентификации

Реквизиты

Документы

Владелец

ФИО Пркоофьева Олеся Алексеевна

СНИЛС

Должность Тест

Почта kgfdgnd@ya.ru

Почта в сертификат kgfdgnd@ya.ru

Телефон +7 999 999-99-99

Реквизиты

Роль Юридическое лицо

Наименование АО "ИИТ"

ИНН 7743020560

КПП 771401001

ОГРН 1027739113049

Адрес г. Москва, г. Москва, ул. Мишина, д. 56, СТР 2, ЭТАЖ, ПОМЕЩ, КОМ 2/IX/11

Процесс

- Проверка данных
- Ожидание оплаты
- Ожидание запроса на сертификат
- Ожидание идентификации**
- Для получения сертификата обратитесь в точку выдачи.
- Подробная информация отправлена на электронную почту kgfdgnd@ya.ru.
- Выпуск сертификата
- Формирование отгрузочных документов
- Ожидание подтверждения завершения
- Завершена

Рисунок 27. Ожидание идентификации

11 Как только вы пройдете идентификацию у ответственного сотрудника, сертификат будет издан и вы сможете установить его (см. [Установка сертификата](#)).

Установка сертификата

После того, как по вашему запросу (см. [Создание запроса на сертификат](#)) будет издан сертификат, вы сможете установить его. Чтобы установить сертификат с помощью вашего криптопровайдера, выполните следующие действия:

- 1 Войдите в Личный кабинет (см. [Вход в программное обеспечение uTrust](#)).
- 2 В списке заявок выберите заявку в статусе «Завершена» и щёлкните на неё (рисунок 28).

Номер	Клиент	Дата подачи	Точка выдачи	Стоимость	Статус	Сертификат
4283	АО "ИИТ": Прокофьева Олеся Алексеевна	04.10.2021	77 - Точка выдачи Корпоративного сценария	Не требует оплаты	Завершена	с 05.10.2021

Рисунок 28. Просмотр списка заявок

- 3 На панели «Процесс» нажмите кнопку «Установить» (рисунок 29).

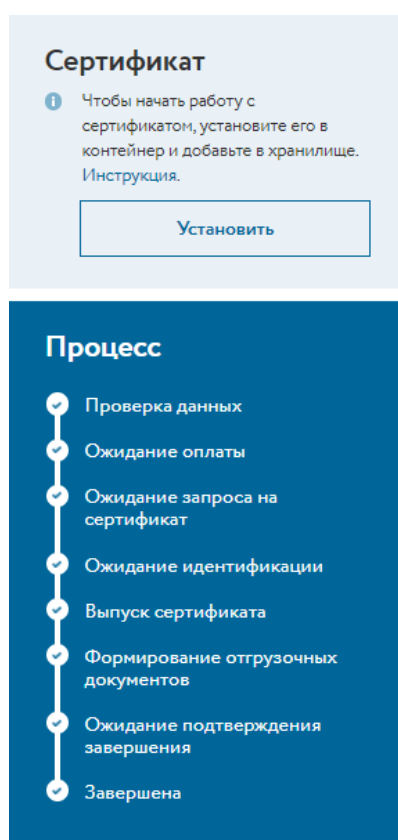


Рисунок 29. Установка сертификата

- 4 В открывшемся окне введите пароль доступа к контейнеру ключей. Если при создании пароля доступа к контейнеру ключей вы не сохраняли пароль, то в зависимости от установленного на вашем компьютере криптопровайдера выполните следующее:
 - в окне криптопровайдера ViPNet CSP установите флажок «Сохранить пароль» и нажмите кнопку «ОК» (рисунок 30).

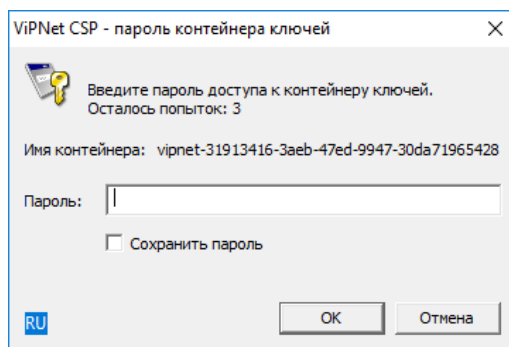


Рисунок 30. Ввод пароля доступа к контейнеру ключей

— в окне криптопровайдера КриптоПро CSP установите флажок «Запомнить пароль» и нажмите кнопку «OK» (рисунок 31).

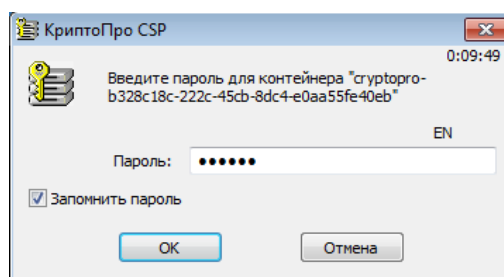


Рисунок 31. Ввод пароля для контейнера ключей

Если вы ввели верный пароль, то вы увидите сообщение об успешной установке сертификата (рисунок 32).

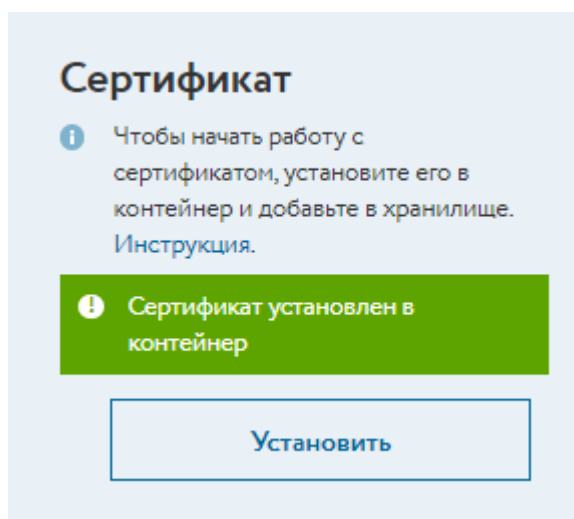


Рисунок 32. Просмотр сообщения «Сертификат успешно установлен»

Глоссарий

Запрос на сертификат

Защищённое электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

Идентификация пользователя

Идентификация, проводимая при личном присутствии пользователя, включающая в себя установление личности владельца сертификата (пользователя) по основному документу, удостоверяющему личность.

Пользователь

Лицо, присоединившееся к регламенту оказания удостоверяющим центром акционерного общества «Инфотекс Интернет Траст» услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей, и зарегистрированное в информационной системе удостоверяющего центра.

Менеджер удостоверяющего центра

Сотрудник удостоверяющего центра, который регистрирует организацию в информационной системе удостоверяющего центра.

Токен

Компактное устройство, предназначенное для обеспечения информационной безопасности пользователя. Также используется для идентификации его владельца, безопасного удалённого доступа к информационным ресурсам и других задач.

Удостоверяющий центр

Акционерное общество «Инфотекс Интернет Траст», осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом «Об электронной подписи».