Настройка автоматизированного рабочего места пользователя для работы с Порталом заявителя информационной системы «Удостоверяющий центр Федерального казначейства»
с использованием ViPNet

**Содержание**

1. [Список сокращений и терминов 2](#_Toc82167667)
2. Общая информация 3
3. [Установка сертификатов 3](#_Toc82167668)
4. [Установка списка аннулированных сертификатов 7](#_Toc82167669)
5. [Проверка включения TLS Unit 11](#_Toc82167670)
6. **Список сокращений и терминов**

|  |  |
| --- | --- |
| **Сокращение, термин** | **Полное наименование, расшифровка** |
| АРМ | Автоматизированное рабочее место |
| ОС | Операционная система |
| ГУЦ | Информационная система головного удостоверяющего центра Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации |
| УЦ ФК | Удостоверяющий центр Федерального казначейства |
| TLS Unit | Компонент для обеспечения организации TLS-соединений со стороны клиента для защищенного доступа к порталам |
| ViPNet PKI Client | Универсальный программный комплекс для работы в инфраструктуре открытых ключей |
| ViPNet CSP | Провайдер криптографических функций |

## **Общая информация**

Для настройки АРМ пользователя для работы с Порталом заявителя информационной системы «Удостоверяющий центр Федерального казначейства» необходимо:

1. Обеспечить на АРМ наличие ОС Windows 7 с пакетом обновления 1 (SP1) и выше, ОС Astra Linux («Астра Линукс»), ОС ГосЛинукс;
2. Обеспечить на АРМ наличие любого Web-браузера с поддержкой криптоалгоритмов ГОСТ: Internet Explorer (версии 9.х, 10.х, 11.х), Яндекс.Браузер ([скачать](https://yandex.ru/promo/browser/general/s/015)), Браузер Chromium ГОСТ ([скачать](https://www.cryptopro.ru/products/chromium-gost)), Google Chrome ([скачать](https://www.google.com/intl/ru/chrome/));
3. Установить сертифицированную версию ViPNet PKI Client версии 1.6 и выше (соответствующую используемой ОС) и ViPNet CSP ([ссылка](https://infotecs.ru/product/all/?line=vipnet-pki)). [Инструкция по установке ViPNet PKI Client](https://infotecs.ru/downloads/documentacii/vipnet-pki-client.html?arrFilter_93=3312508659&set_filter=Y);
4. Установить драйвера ключевого носителя (например: Рутокен ([скачать](https://www.rutoken.ru/support/download/windows/)), e-Token ([скачать](https://www.aladdin-rd.ru/support/downloads));
5. Установить сертификаты Минцифры России (ГУЦ) и УЦ ФК (описание процесса установки описано ниже);
6. Установить список аннулированных сертификатов (описание процесса установки описано ниже).

***Примечание****. Данная настройка обязательна для построения цепочки сертификатов в случае установки личного сертификата с помощьюViPNet PKI Client*.

1. Проверить включение TLS Unit на АРМ.

## **Установка сертификатов**

С целью дальнейшей установки сертификатов на АРМ пользователя необходимо предварительно сохранить их себе на жесткий диск. Для этого:

1. Открыть веб-браузер и перейти на официальный сайт Федерального казначейства <http://www.roskazna.gov.ru/>
2. Перейти в раздел ГИС/Удостоверяющий центр/Корневые сертификаты (<https://www.roskazna.gov.ru/gis/udostoveryayushhij-centr/kornevye-sertifikaty/>). Сертификаты ГУЦ и УЦ ФК расположены на вкладке «2022»,
3. Активировать ссылку на скачивание сертификатов:
* Ссылка на скачивание сертификата ГУЦ - <https://roskazna.gov.ru/upload/iblock/f5e/Kornevoy-sertifikat-GUTS-2022.CER>
* Ссылка на скачивание сертификата УЦ ФК 2022 года - <https://roskazna.gov.ru/upload/iblock/1af/Kaznacheystvo-Rossii.CER> На предложение сохранить файл сертификата выбрать локальную директорию в АРМ пользователя, в которую необходимо сохранить файл.
1. Сохранить файл сертификата.

**Установка сертификатов Минцифры России (ГУЦ) и УЦ ФК осуществляется по одному и тому же алгоритму через настройки ViPNet PKI Client.**

После загрузки файлов сертификатов себе на АРМ необходимо:

1. Открыть настройки ViPNet PKI Client (Рисунок 1).



Рисунок 1 - Окно настроек ViPNet PKI Client

1. Перейти к вкладке «Сертификаты» (Рисунок 2).



Рисунок 2 - Окно настроек ViPNet PKI Client вкладка «Сертификаты»

1. Нажать «Добавить сертификат или CRL» (Рисунок 3).



Рисунок 3 - Кнопка добавления сертификата

1. В появившемся окне выбрать сохраненный ранее на АРМ файл сертификата.
2. На форме добавления сертификатов нажать «Добавить» *(Обращаем внимание, что тип сертификата ViPNet-ом определяется автоматически и никаких дополнительных действий от пользователя не требуется)* (Рисунок 4).



Рисунок 4 - Добавления сертификата

После добавления сертификата пользователь увидит сообщение об успешном добавлении сертификата (Рисунок 5).



Рисунок 5 - Подтверждение успешной установки сертификата

Нажать «Закрыть».

В результате на АРМ пользователя будет успешно установлен сертификат.

## **4. Установка списка аннулированных сертификатов**

С целью дальнейшей установки списков отозванных сертификатов на АРМ пользователя необходимо предварительно сохранить их себе на жесткий диск. Для этого:

1. Открыть веб-браузер и перейти по ссылке для скачивания списка отозванных сертификатов УЦ ФК <http://crl.roskazna.ru/crl/>
2. Активировать ссылку на скачивание списка отозванных сертификатов.
* Ссылка на скачивание списка отозванных сертификатов ГУЦ - <http://rostelecom.ru/cdp/guc2022.crl>
* Ссылка на скачивание списка отозванных сертификатов удостоверяющего центра Федерального казначейства 2022 года - <http://crl.roskazna.ru/crl/ucfk_2022.crl>
1. На предложение сохранить файл списка отозванных сертификатов выбрать локальную директорию в АРМ пользователя, в которую необходимо сохранить файл.
2. Сохранить файл списка отозванных сертификатов.

**Установка всех списков аннулированных сертификатов осуществляется по одному и тому же алгоритму через настройки ViPNet PKI Client.**

После загрузки файлов себе на АРМ необходимо:

1. Открыть настройки ViPNet PKI Client (Рисунок 6).



Рисунок 6 - Установка списка аннулированных сертификатов.

Окно настроек ViPNet PKI Client

1. Перейти к вкладке «Сертификаты» (Рисунок 7).



Рисунок 7 - Установка списка аннулированных сертификатов. Окно настроек
ViPNet PKI Client вкладка «Сертификаты»

1. Нажать «Добавить сертификат или CRL» (Рисунок 8)



Рисунок 8 - Добавление CRL

1. В появившемся окне выбрать сохраненный ранее на АРМ файл списка отозванных сертификатов.
2. На форме добавления сертификатов нажать «Добавить» *(Обращаем внимание, что тип списка отозванных сертификатов ViPNet-ом определяется автоматически и никаких дополнительных действий от пользователя не требуется)* (Рисунок 9).



Рисунок 9 – Добавление списка аннулированных сертификатов

После добавления списка аннулированных сертификатов пользователь увидит сообщение об успешном добавлении сертификата (Рисунок 10).



Рисунок 10 - Подтверждение успешной установки списка аннулированных сертификатов

Нажать «Закрыть».

В результате на АРМ пользователя будет успешно установлен список аннулированных сертификатов.

## **5. Проверка включения TLS Unit**

Для корректной работы с Порталом заявителя обязательно включение TLS Unit в настройках ViPNet PKI Client.

При установке ViPNet PKI Client TLS Unit включается автоматически, однако для исключения ошибки рекомендовано проверить успешность настройки. Для проверки включения необходимо:

1. Открыть настройки ViPNet PKI Client (Рисунок 11)



Рисунок 11 – Проверка включения TLS.Окно настроек ViPNet PKI Client

1. Перейти к настройкам TLS (Рисунок 12)



Рисунок 12 - Окно настроек ViPNet PKI Client вкладка «TLS»

1. Проверить включение TLS Unit и Разрешения соединения при неполном доверии к сертификату сервера (Рисунок 13)



Рисунок 13 - Проверка включения TLS

Если TLS Unit не включен, его требуется включить по алгоритму:

* Изменить состояние переключателя включения/выключения TLS Unit и включить настройку «Разрешить соединения при неполном доверии к сертификату сервера» (если не включена) (Рисунок 14).



Рисунок 14 - Включение TLS

* В случае необходимости нажать «Сохранить» (Рисунок 15)



Рисунок 15 - Сохранение настроек TLS

***Примечание.*** *Если включение TLS Unit завершилось неуспешно, необходимо обратиться к специалистам Инфотекс.*