Инструкция по созданию ключевой пары и PKCS#10 запроса на сертификат с применением сертифицированного СКЗИ ViPNet CSP

Оглавление

Введение

Инструкция предназначена для налогоплательщиков: Единолично исполнительного органа общества (генеральный директор, президент и другие) Юридического лица (ЕИО ЮЛ) или Индивидуального предпринимателя (ИП), самостоятельно формирующих: ключ электронной подписи, ключ проверки электронной подписи, запрос на получение сертиката формата PKCS#10 с использованием бесплатного сертифицированного СКЗИ ViPNet CSP для последующего получения квалифицированного сертификата ключа проверки электронной подписи в удостоверяющем центре федерального налоговой службе РФ. В соответствии с пунктом 11 Порядка реализации ФНС России функций аккредитованного удостоверяющего центра, утвержденного приказом ФНС России от 30.12.2020 № ВД-7-24/982@ и зарегистрированного Минюстом России 14.05.2021 № 63416 (далее – Порядок) в УЦ ФНС России - допускается самостоятельное формирование ключа электронной подписи и ключа проверки электронной подписи (далее – ключевой пары) заявителем с использованием собственных сертифицированных средств криптографической защиты информации. Сформированный при этом файл запроса формата PKCS#10 на выпуск квалифицированного сертификата предоставляется в налоговый орган, оказывающий услугу по выдаче квалифицированной электронной подписи, на съемном носителе информации – флэш накопителе (USB Тип А)[1].

[1] Согласно официального разъяснения ЗГ-3-24/11708@ от 25.10.2022 Начальника управления информационной безопасности УЦ ФНС РФ В.А. Суховецкого по запросу № 045423/ЗГАО от 20.10.2022 от АО ИИТ о возможных способах физической передачи PKCS#10 запроса налогоплательщиком при личном присутствии в ФНС в случаях, когда ключевая пара создается самостоятельно на АРМ налогоплательщика с применением сертифицированного СКЗИ.

Получение и установка ViPNet CSP

Для создания запроса необходимо установить криптопровайдер ViPNet CSP версии 4.4.4 и выше. Для получения ViPNet CSP необходимо перейти на официальный сайт разработчика по адресу https://infotecs.ru/products/vipnet-csp и скачать актуальную версию. Файлы доступны для скачивания только авторизованным пользователям. Необходимо пройти регистрацию на сайте и авторизоваться.

Подробную информацию по установке и регистрации СКЗИ ViPNet CSP можно найти в инструкции https://iitrust.ru/downloads/manual/general/Setting_PM_JaCarta.pdf (раздел II).

Установка драйверов (ПО) для USB токенов

Следующим этапом после установки СКЗИ ViPNet CSP необходимо подключить токен и установить для него драйвера (ПО) с официального сайта согласно производителю:

- Для устройств JaCarta LT, JaCarta-2 SE, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta PKI произведите установку программного обеспечения для ключевых носителей JaCarta;
- Для устройств Рутокен S, Рутокен Lite, Рутокен ЭЦП 3.0, произведите установку программного обеспечения для ключевых носителей Рутокен;
- Для устройств ESMART Token, ESMART Token ГОСТ, произведите установку программного обеспечения для ключевых носителей ESMART Token.

Создание запроса PKCS#10

1. Для создания запроса необходимо через меню Пуск найти раздел ***«ViPNet»*** и нажать на пункт ***«Создание запроса на сертификат»*** (Рисунок 1).

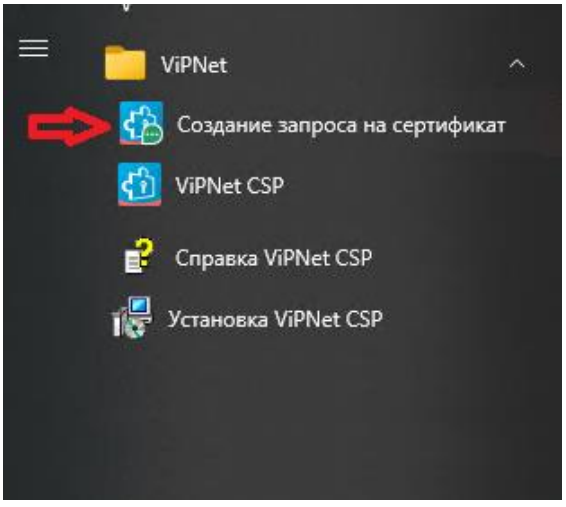

Рисунок 1

2. После запуска утилиты необходимо настроить ***Параметры сертификата*** согласно рекомендациям (Рисунок 2)

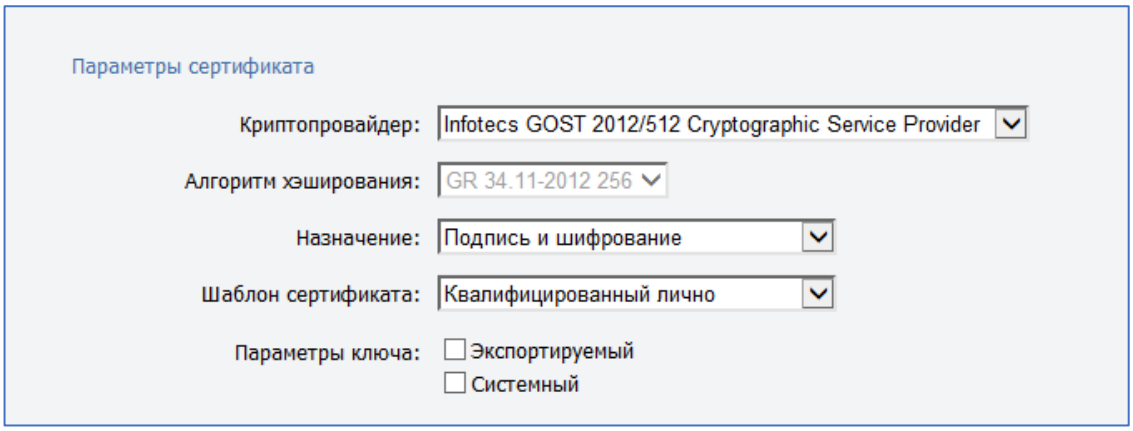

Рисунок 2

3. Далее необходимо заполнить Данные о владельце сертификата согласно категории заявителя (ИП или ЮЛ) (Рисунок 3).

Во избежание ошибок по требованиям к форме квалифицированного сертификата ключа проверки электронной подписи утвержденные приказом ФСБ России от 27 декабря 2011 г. № 795 - рекомендуем заполнять (копировать) реквизиты ЮЛ/ИП в поля окна (рисунок 3) из актуальной выписки ЕГРЮЛ/ЕГРИП, которую можно получить на сайте ФНС https://egrul.nalog.ru/index.html

---

Заполните реквизиты в форме создания запроса на сертификат, чтобы не допустить ошибки. Обратите внимание как заполнять формат поля «Область».

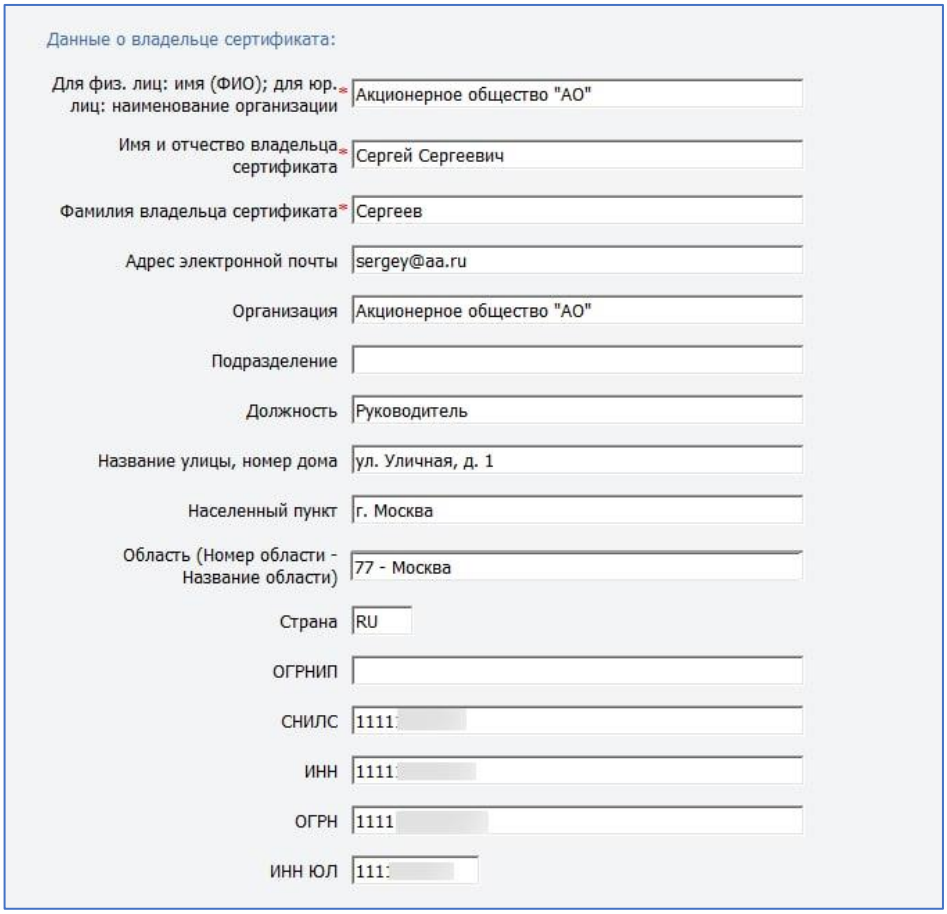

Рисунок 3

4. В поле сохранения запроса (Рисунок 4) необходимо либо запомнить предлагаемый путь по умолчанию, либо через клавишу ***«Обзор»*** выбрать удобное место сохранения запроса,

например, сразу указать путь до USB Flash[2] *(данный файл *.p10 не является закрытым ключом и потребуется для передачи в УЦ ФНС - на основании него будет выпускаться сертификат)* и нажать ***«Сформировать запрос»***.

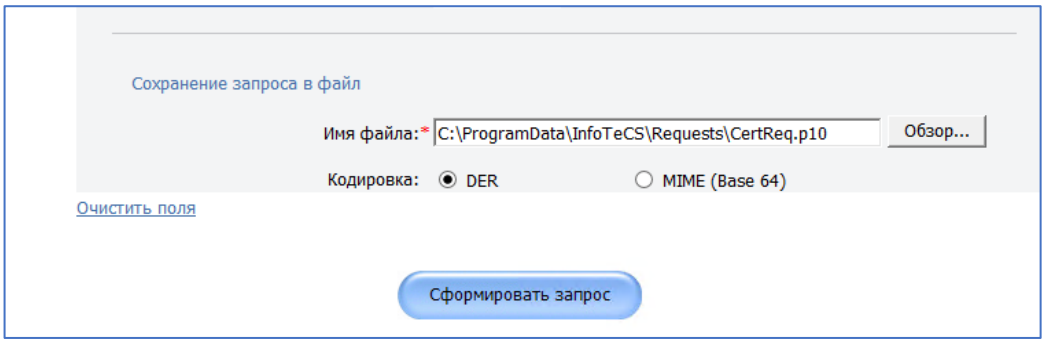

Рисунок 4

5. После нажатия на ***«Сформировать запрос»*** появится окно «ViPNet CSP – инициализация контейнера ключей» (Рисунок 5), в котором будет автоматически сформировано имя контейнера ключа *(имя контейнера можно переименовать, это не влияет на дальнейшую работу)*. В соответствии требованиям УЦ ФНС[3] в качестве места хранения рекомендуется выбрать подключенный ранее USB токен и ввести пин-код (указывается в документах/сертификате при покупке защищенного носителя).

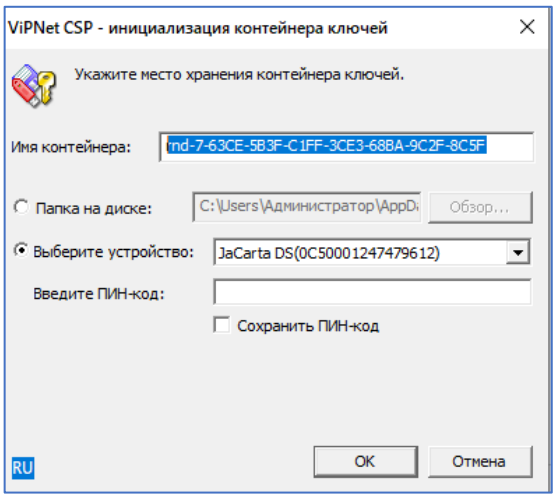

Рисунок 5

6. В окне «Электронная рулетка» поводите мышкой в пределах появившегося окна или нажимайте различные клавиши на клавиатуре, пока индикатор не достигнет 100% (Рисунок 6).

[2] Рекомендуем заранее отформатировать USB Flash, на которую затем будете сохранять файл PKCS#10 запроса;

[3] В соответствии с пунктом 22 порядка реализации ФНС функций аккредитованного УЦ и исполнения его обязанностей утверждённого Приказом ФНС России от 30.12.2020 N ВД-7-24/982@ для формирования ключа ЭП в качестве средства ЭП заявителем используются носители ключевой информации, сертифицированные федеральным органом исполнительной власти в области обеспечения безопасности *(JaCarta LT, JaCarta-2 SE, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta PKI;Рутокен ЭЦП 2.0, Рутокен Lite, Рутокен S;ESMART Token, ESMART Token ГОСТ)*.

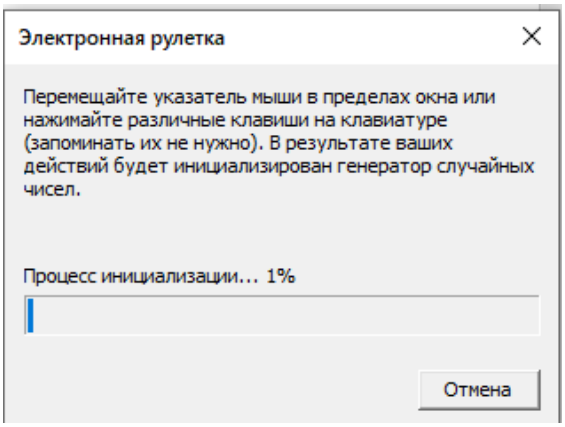

Рисунок 6

7. После выполнения процесса инициализации «Электронной рулетки» появится окно (Рисунок 7) с текстом «Сертификационный запрос создан успешно». Данное окно будет свидетельствовать о том, что запрос успешно создан и сохранен в указанную ранее папку, а контейнер электронной подписи (закрытый ключ) успешно размещен в секции памяти токена. Необходимо нажать ***«ОК»***.

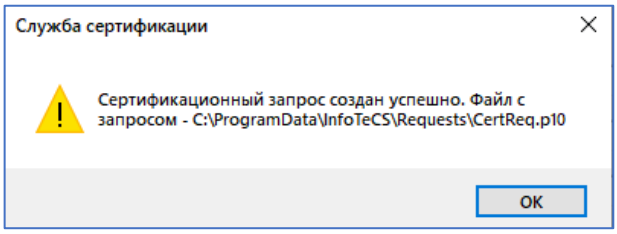

Рисунок 7

8. Для получения сертификата обратитесь в УЦ ФНС России или к доверенному лицу УЦ ФНС России с необходимыми документами, USB-носителем с файлом запроса, токеном с сохраненным контейнером ключа, а также памяткой (см. «Памятка налогоплательщика для получения КСКПЭП в УЦ ФНС России по PKCS#10 запросу»).

9. После получения квалифицированного сертификата ключа проверки электронной подписи в УЦ ФНС согласно приведенной инструкции и возникновении сложностей эксплуатации и его применения в информационных системах Вы можете обратиться в АО ИнфоТеКС Интернет Траст за разовыми услугами настройки электронной подписи или годовой подпиской на настройку и квалифицированное техническое сопровождение полученного сертификата. Обратиться можно по телефону 88002508265 (звонок бесплатный) или электронной почте 77@iitrust.ru.