

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

Оглавление

Введение	3
Получение и установка ViPNet CSP	4
Установка драйверов (ПО) для USB токенов.....	4
Создание запроса PKCS#10.....	4

Введение

Инструкция предназначена для налогоплательщиков: Единоличного 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 сертификата формата PKCS#10 с использованием бесплатного [сертифицированного СКЗИ ViPNet CSP](#) для последующего получения квалифицированного сертификата ключа проверки электронной подписи в удостоверяющем центре федеральной налоговой службы России. 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 СКЗИ ViPNet CSP версии 4.4.2 и выше:

- Если вы работаете на операционных системах Windows 10/11, вам необходимо перейти по адресу https://infotecs.ru/downloads/latest/?product=vipnet_csp&type=beta для получения дистрибутива ViPNet CSP поддерживаемой данными ОС.
- Если вы работаете на операционной системе Windows: 8.1/Server 2008/Server 2008 R2/Server 2012/Server 2012R2/2016/2019, вам необходимо перейти по адресу https://infotecs.ru/downloads/latest/?product=vipnet_csp&type=full для получения дистрибутива ViPNet CSP поддерживаемой данными ОС.

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-2 SE, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, произведите установку [программного обеспечения для ключевых носителей JaCarta](#);
- Для устройств Рутокен ЭЦП 2.0, произведите установку [программного обеспечения для ключевых носителей Рутокен](#);
- Для устройств 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).

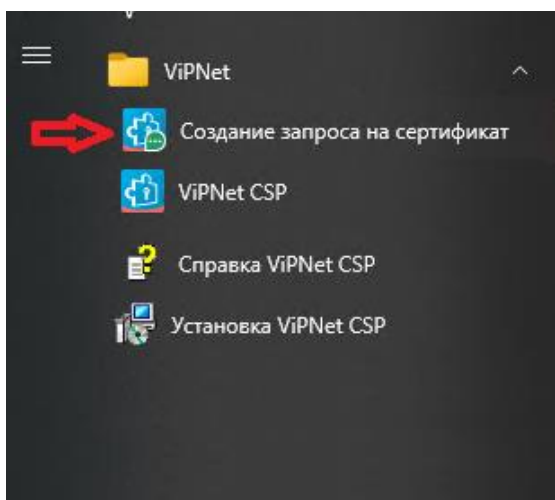


Рисунок 1

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

Параметры сертификата

Криптопровайдер: Infotecs GOST 2012/512 Cryptographic Service Provider

Алгоритм хэширования: GR 34.11-2012 256

Назначение: Подпись и шифрование

Шаблон сертификата: Квалифицированный лично

Параметры ключа: Экспортируемый
 Системный

Рисунок 2

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

i Во избежание ошибок к [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».

Данные о владельце сертификата:

Для физ. лиц: имя (ФИО); для юр. лиц: наименование организации: Акционерное общество "АО"

Имя и отчество владельца сертификата: Сергей Сергеевич

Фамилия владельца сертификата: Сергеев

Адрес электронной почты: sergey@aa.ru

Организация: Акционерное общество "АО"

Подразделение:

Должность: Руководитель

Название улицы, номер дома: ул. Уличная, д. 1

Населенный пункт: г. Москва

Область (Номер области - Название области): 77 - Москва

Страна: RU

ОГРНИП:

СНИЛС: 1111

ИНН: 1111

ОГРН: 1111

ИНН ЮЛ: 111

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, можно сразу указать путь до USB Flash² (*данный файл *.p10 не является закрытым ключом и потребуется для передачи в УЦ ФНС - на основании него будет выдан сертификат*). Нажать **«Сформировать запрос»**.

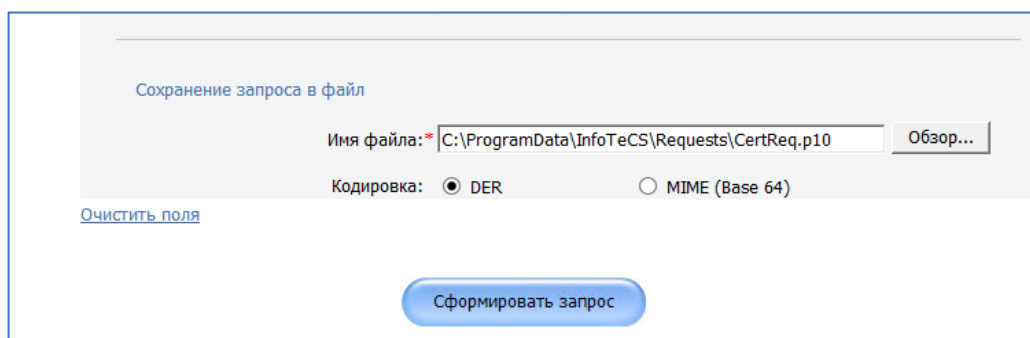


Рисунок 4

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 с требованиями УЦ ФНС³ в качестве места хранения контейнера ключей рекомендуется выбрать [подключенный ранее](#) USB токен и ввести пинкод (*указывается в документах/сертификате при покупке защищенного носителя*). В случае если применяется устройство *JaCarta-2 PKI/ГОСТ*, то в поле «Выберите устройство» высветится три типа устройства:
- чтобы ключевая пара была сгенерирована встроенным аппаратным СКЗИ токена в ГОСТ секции - необходимо выбрать «JaCarta GOST 2.0» (рисунок 5, позиция Б).
 - чтобы ключевая пара была сгенерирована программным СКЗИ ViPNet CSP – нужно выбрать «JaCarta Laser»⁴ (рисунок 5, позиция А).

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-2 SE, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0, ESMART Token ГОСТ*).

⁴ В этом случае ключевая пара сгенерируется в PKI секции устройства JaCarta-2 PKI/ГОСТ и контейнер закрытого ключа будет формата ViPNet CSP, при этом в УЦ ФНС могут возникнуть сложности при записи квалифицированного ключа проверки электронной подписи сразу на это устройство, если рабочее место сотрудника ФНС не оборудовано для работы с СКЗИ ViPNet CSP/ViPNet PKI Client [см. информацию в памятке](#).

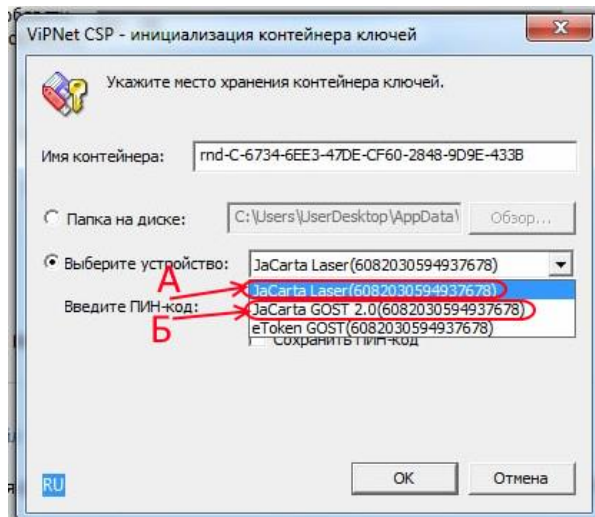


Рисунок 5

6. Если на 5 шаге было выбрано устройство «JaCarta Laser» (рисунок 5, позиция А) то для генерации ключевой пары появится окно «Электронная рулетка» в котором необходимо поводить мышкой в пределах появившегося окна или нажимайте различные клавиши на клавиатуре, пока индикатор не достигнет 100% (Рисунок 6).

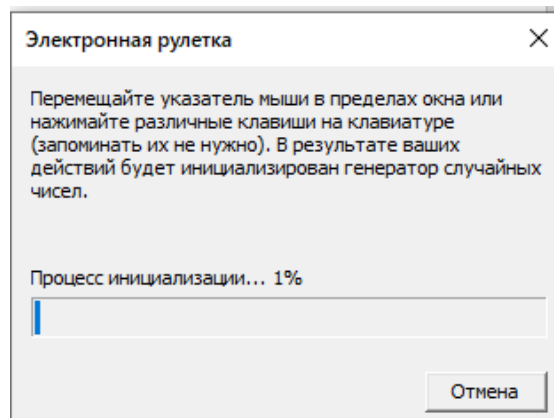


Рисунок 6

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**».

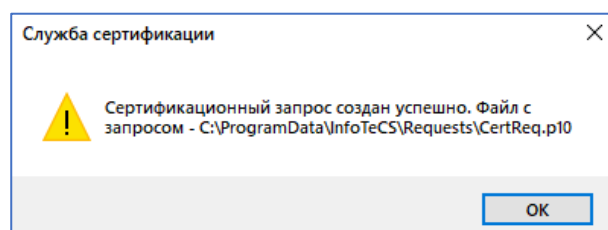


Рисунок 7

8. Если на 5 шаге было выбрано устройство «JaCarta GOST 2.0» (рисунок 5, позиция Б), либо используется сертифицированный ФСБ носитель другого вендора (*Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0, ESMART Token ГОСТ*), то окно «Электронная рулетка» не появится, так как генерация ключевой пары будет происходить аппаратным СКЗИ токена, при успешном завершении генерации появится окно «Служба сертификации» (рисунок 7) с информацией

о успешном завершении создания запроса, в котором необходимо нажать «ОК» и перейти к 9 шагу

9. Для получения сертификата обратитесь в [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»](#)).
10. 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.