**Подключение к API ЕНС**

**Оглавление**

[1. Введение 3](#_Toc153383127)

[1.1 Общие положения 3](#_Toc153383128)

[1.2 Список терминов и сокращений 3](#_Toc153383129)

[2. Описание процесса подключения к API ЕНС 6](#_Toc153383130)

[2.1 Требования к клиенту ЕНС 6](#_Toc153383131)

[2.2 Квалифицированная электронная подпись 8](#_Toc153383132)

[2.2.1 Что такое квалифицированная электронная подпись? 8](#_Toc153383133)

[2.2.2 Получение квалифицированной электронной подписи 8](#_Toc153383134)

[2.3 Машиночитаемая доверенность 9](#_Toc153383135)

[2.3.1 Что такое машиночитаемая доверенность? 9](#_Toc153383136)

[2.3.2 Получение машиночитаемой доверенности 9](#_Toc153383137)

[2.4 Взаимодействие через оператора ВУС 10](#_Toc153383138)

[3. Настройка подключения к API ЕНС 10](#_Toc153383139)

[3.1 Настройка окружения 10](#_Toc153383140)

[3.2 Аутентификация и подключение к сервису ЕНС 11](#_Toc153383141)

[3.3 Доступ к API ЕНС 11](#_Toc153383142)

1. **Введение**
	1. **Общие положения**

Данный документ содержит описание требований к клиенту ЕНС, а также процесса подключения к API ЕНС.

* 1. **Список терминов и сокращений**

| **Термин или сокращение** | **Описание** |
| --- | --- |
| Белый IP-адрес | IP-адрес, под которым компьютер, ноутбук, планшет, телефон или иное устройство видно и работает в Интернете |
| ГОСТ | Государственный стандарт |
| ЕНП | Единый налоговый платеж |
| ЕНС | Единый налоговый счет |
| ИП | Индивидуальный предприниматель |
| Квалифицированный сертификат | Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра, соответствующий требованиям, установленным ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи |
| Клиент ЕНС | Физическое лицо, юридическое лицо или индивидуальный предприниматель, который использует API ЕНС или имеет намерение использовать его для получения информации о состоянии своего единого налогового счета или единого налогового счета того лица-доверителя или той организации-доверителя, доверенным лицом которой он является |
| Ключ электронной подписи | Уникальная последовательность символов, предназначенная для создания электронной подписи |
| КЭП | Квалифицированная электронная подпись |
| МЧД | Машиночитаемая доверенность |
| НП | Налогоплательщик |
| Оператор ВУС | Организация, которая обеспечивают юридически значимый электронный документооборот между налогоплательщиком и налоговым органом |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| РФ | Российская Федерация |
| Сессионный токен | Зашифрованная последовательность символов, которая позволяет точно идентифицировать объект и определить уровень его привилегий. Сессионный токен генерируется системой авторизации и привязывается к конкретному сеансу работы, клиенту сети или пакету данных |
| Средства электронной подписи | Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи |
| ТКС | Телекоммуникационный канал связи |
| УЦ | Удостоверяющий центр |
| ФЗ | Федеральный закон |
| ФЛ | Физическое лицо |
| ФНС | Федеральная налоговая служба |
| ФСБ | Федеральная служба безопасности |
| ФСТЭК | Федеральная служба по техническому и экспортному контролю |
| ЮЛ | Юридическое лицо |
| API | Application Programming Interface (программный интерфейс приложения) - интерфейс прикладного программирования, который представляет собой набор готовых классов, процедур, функций, структур и констант, которые предоставляются сервисом для использования во внешних программных продуктах |
| HTTP | HyperText Transfer Protocol (протокол передачи гипертекста) - протокол прикладного уровня, предназначенный для передачи данных в интернете |
| HTTP-заголовок | Поле HTTP-запроса или ответа, которое передает дополнительный контекст и метаданные о запросе или ответе |
| HTTP-запрос | Сообщение, которое отправляется клиентом на сервер, чтобы вызвать выполнение некоторых действий |
| IP-адрес | Уникальный адрес, идентифицирующий устройство в интернете или локальной сети |
| TLS | Transport Layer Security (протокол защиты транспортного уровня) - протокол, поддерживающий защищенную передачу данных между клиентом и сервером |
| URL | Uniform Resource Locator (Унифицированный указатель ресурса) - адрес ресурса в сети Интернет |
| XML | eXtensible Markup Language (расширяемый язык разметки) - язык разметки, предназначенный для хранения и передачи данных |

1. **Описание процесса подключения к API ЕНС**
	1. **Требования к клиенту ЕНС**

Для подключения к API ЕНС и последующей работы с ним клиент ЕНС должен соответствовать следующим требованиям:

1. Если взаимодействие будет осуществляться через оператора ВУС, то у клиента должно быть настроено взаимодействие через выбранного оператора, а также подано согласие налогоплательщика (плательщика страховых взносов) на представление налоговым органом сведений о налогоплательщике (плательщике страховых взносов), составляющих налоговую тайну, иному лицу (оператору) через API ЕНС;
2. Клиент ЕНС и/или оператор ВУС должен иметь действующую КЭП. КЭП должна быть выпущена в формате CAdES-BES (PKCS#7) по ГОСТ 34.10-2012 (256);
3. Если НП хочет предоставить возможность получать данные о состоянии ЕНС другому ФЛ, то в таком случае необходимо получить машиночитаемую доверенность.

После выполнения вышеперечисленных условий клиент может произвести настройку подключения к API ЕНС. Схема процесса подключения к API ЕНС представлена ниже.



* 1. **Квалифицированная электронная подпись**
		1. **Что такое квалифицированная электронная подпись?**

Квалифицированная электронная подпись (КЭП) - электронная подпись, которая соответствует следующим признакам:

1. Получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
2. Ключ проверки электронной подписи указан в квалифицированном сертификате;
3. Для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с ФЗ № 63-ФЗ от 06.04.2011 «Об электронной подписи».

КЭП используется для следующих целей:

1. Подтверждает юридическую силу подписанного документа;
2. Позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
3. Помогает определить лицо, подписавшее электронный документ.
	* 1. **Получение квалифицированной электронной подписи**

Для получения КЭП ФЛ необходимо обратиться в удостоверяющий центр, [аккредитованный Министерством цифрового развития, связи и](https://digital.gov.ru/ru/activity/govservices/certification_authority/?utm_referrer=https%3a%2f%2fca.kontur.ru%2f&utm_referrer=https%3a%2f%2fdigital.gov.ru%2fru%2factivity%2fgovservices%2fcertification_authority%2f%3futm_referrer%3dhttps%253a%252f%252fca.kontur.ru%252f) [массовых коммуникаций Российской Федерации,](https://digital.gov.ru/ru/activity/govservices/certification_authority/?utm_referrer=https%3a%2f%2fca.kontur.ru%2f&utm_referrer=https%3a%2f%2fdigital.gov.ru%2fru%2factivity%2fgovservices%2fcertification_authority%2f%3futm_referrer%3dhttps%253a%252f%252fca.kontur.ru%252f) и предоставить следующие документы:

1. Основной документ, удостоверяющий личность (паспорт);
2. Документ о страховом номере индивидуального лицевого счета (СНИЛС).

Руководители организаций (лица, имеющие право действовать от имени ЮЛ без доверенности) и ИП должны руководствоваться порядком получения КЭП, опубликованном на [сайте ФНС России](https://www.nalog.gov.ru/rn77/related_activities/ucfns/el_sign_getting/).

Для этого необходимо предоставить:

1. Основной документ, удостоверяющий личность (паспорт);
2. Документ о страховом номере индивидуального лицевого счета (СНИЛС);
3. Сведения об идентификационном номере налогоплательщика (ИНН) ФЛ и (или) ЮЛ;
4. USB-токен, сертифицированный ФСБ России или ФСТЭК России. Можно предоставить уже использующийся токен, если он имеет действующий сертификат соответствия ФСТЭК или ФСБ России.
	1. **Машиночитаемая доверенность**
		1. **Что такое машиночитаемая доверенность?**

МЧД – это электронная форма бумажной доверенности, подтверждающей полномочия представителя НП, подписанная КЭП руководителя организации или ИП. МЧД создается и представляется в файле формата XML.

Данную доверенность получает НП и передает тому ФЛ, которое будет действовать от имени данного НП.

* + 1. **Получение машиночитаемой доверенности**

Для получения МЧД необходимо обратиться в [УЦ ФНС России](https://www.nalog.gov.ru/rn77/related_activities/ucfns/). Также оформить МЧД можно на сайте ФНС России с помощью сервиса [«Создание и проверка доверенности в электронной форме»](https://service.nalog.ru/dovel/#/). Сервис позволяет сформировать МЧД в виде файла, скачать его, и в дальнейшем использовать по назначению.

Для оформления МЧД необходимо предоставить следующие данные:

1. Если доверитель – руководитель российской организации, то необходимо предоставить:
	1. Наименование и адрес организации;
	2. ИНН;
	3. ОГРН ЮЛ;
	4. КПП;
	5. Данные о доверителе (лице, которое действует от имени организации без доверенности):
		* должность;
		* ФИО;
		* ИНН;
		* СНИЛС;
		* дату рождения;
	6. Данные о доверенном лице:
		* ФИО;
		* ИНН;
		* ОГРНИП, если доверенным лицом является ИП;
		* СНИЛС;
		* дату рождения;
		* основной документ, удостоверяющий личность (паспорт).
2. Если доверитель - ИП, то необходимо предоставить:
	1. ФИО;
	2. дату рождения;
	3. основной документ, удостоверяющий личность (паспорт);
	4. СНИЛС;
	5. ИНН;
	6. ОГРНИП.
	7. **Взаимодействие через оператора ВУС**

Для взаимодействия с API ЕНС через оператора ВУС клиенту необходимо заключить договор на оказание услуг с выбранным оператором, произвести настройку необходимого ПО и (или) оборудования и предоставить согласие на представление налоговым органом сведений о налогоплательщике, составляющих налоговую тайну, иному лицу или признание таких сведений общедоступными.

ЮЛ и ИП могут направить данное согласие по ТКС или через личный кабинет. С форматом и порядком представления согласия можно ознакомиться на [сайте ФНС России](https://www.nalog.gov.ru/rn77/taxation/privacy/).

Версия формата согласия должна быть 5.03.

При заполнении согласия налогоплательщика (плательщика страховых взносов) на представление налоговым органом сведений о налогоплательщике (плательщике страховых взносов), составляющих налоговую тайну, иному лицу (оператору) через API ЕНС необходимо указать:

1. ИНН лица, которому НП раскрывает свои сведения;
2. В поле «Код комплекта сведений» указать значение 21001;
3. В поле «Признак представления сведений» указать значение 2.
4. **Настройка подключения к API ЕНС**

Для подключения к API ЕНС клиенту необходимо:

1. Настроить окружение для взаимодействия через протокол TLS с использованием алгоритма ГОСТ или RSA;
2. Пройти аутентификацию для получения токена доступа (сессионного токена) и обратиться к сервису ЕНС.
	1. **Настройка окружения**

Для взаимодействия через протокол TLS с использованием алгоритма RSA необходимо установить следующее ПО:

1. OpenJDK;
2. КриптоПРО JCP v.2.0.42644-81dc08c9 от 2022г.;
3. При помощи штатной панели управления КриптоПРО JCP: `ControlPanel.bat` или `ControlPanel.sh` (в зависимости от ОС), установить в хранилище HDImageStore связку: закрытый ключ и сертификат.

Сертификат должен удовлетворять следующим требованиям:

1. В сертификате должен присутствовать атрибут с ИНН;
2. Сертификат должен быть применим для формирования ЭЦП по стандарту ГОСТ 34.10-2012 (256);
3. Количество сертификатов в ЭЦП должно быть не больше одного;
4. Сертификат актуален на момент проверки.
	1. **Аутентификация и подключение к сервису ЕНС**

Для обращения к API ЕНС необходимо пройти предварительную аутентификацию, в результате которой получить токен доступа (сессионный токен). Сессионный токен потребуется указывать в специализированном заголовке при обращении к API ЕНС.

Прохождение аутентификации:

1. Клиент, пользуясь синхронным сервисом сообщений, на предоставленный ФНС адрес сервиса получения временного ключа направляет HTTP-запрос для получения временного (одноразового) ключа. В ответ возвращается временный (одноразовый) ключ, а также время его деактивации.
2. Клиент, пользуясь синхронным сервисом сообщений, на предоставленный ФНС адрес сервиса аутентификации по цифровой подписи с квалификационным сертификатом направляет HTTP-запрос, передавая полученный временный ключ и подписанное значение временного ключа средствами КЭП (подпись: CAdES-BES, алгоритм: ГОСТ 2012 256) закодированного алгоритмом BASE64. В ответ возвращается токен доступа (сессионный токен) и период его действия.

Для обращения к API ЕНС необходимо указывать в специализированном заголовке полученный сессионный токен, закодированный алгоритмом Base64-URL.

* 1. **Доступ к API ЕНС**

Доступ к API ЕНС осуществляется только по белым IP-адресам. Для получения технической документации и доступа необходимо направить по адресу: utaapi@gnivc.ru с темой письма **«Доступ для подключения к API»** следующие данные:

1. ИНН;
2. Наименование ЮЛ или ИП;
3. Контактную информацию: ФИО, телефон, e-mail (в домене организации);
4. Перечень белых IP-адресов.

Для доступа к API ЕНС используется URL [http://dpc.tax.nalog.ru](http://dpc.tax.nalog.ru/).