

Pert

Техническая документация

Table of contents

1. Главная	3
1.1 Документация системы	3
2. Интеграция	4
2.1 Начало работы	4
2.2 Авторизация	6

1. Главная

1.1 Документация системы

Добро пожаловать в документацию системы Pert.

2. Интеграция

2.1 Начало работы

Это краткое руководство поможет вам шаг за шагом: создать API-ключ и выполнить первые запросы к Pert API.

В итоге вы сможете: - создать и подтвердить API-пользователя - создать vault-аккаунт - отправить свою первую транзакцию

Как работает аутентификация API

Pert использует асимметричную криптографию для защиты взаимодействия с API. Проще говоря, это работает так:

Компонент	Описание
Секретный API-ключ (приватный ключ)	Хранится только у вас и используется для подписи авторизационного запроса, чтобы подтвердить, что он отправлен именно вами
Публичный ключ	Находится у Pert и нужен для проверки, что запрос действительно подписан вашим приватным ключом

Такая архитектура гарантирует, что ваш секретный API-ключ **никогда** не покидает ваше окружение — в Pert передаётся только публичный ключ. Мы не можем подписывать запросы за вас, и даже в случае компрометации системы Pert ваши учётные данные останутся в безопасности.

Шаг 1: Генерация пары ключей

В каждом запросе к API Pert должен передаваться авторизационный JWT-токен:

Заголовок	Значение
Authorization	Bearer <code>JWT_TOKEN</code>

Для получения авторизационного JWT-токена необходимо отправить запрос подписанный асимметричным ключом шифрования.

Используйте OpenSSL для генерации пары ключей `ed25519`

```
# генерируем приватный ключ
openssl genpkey -algorithm ED25519 -out "pert_secret.pem"

# генерируем публичный ключ
openssl pkey -in "pert_secret.pem" -pubout -out "pert_public.pem"
```

В результате выполнения этой команды создаются:

- **pert_secret.pem** — ваш приватный Ed25519-ключ, который используется как API-секрет
- **pert_public.pem** — файл публичного ключа, который нужно будет загрузить при создании API-ключа

Обязательно храните файл с секретным ключом в надёжном и безопасном месте.

Шаг 2: Создание API-пользователя

Чтобы создать API-пользователя с правами подписи, выполните следующие шаги:

- В консоли Pert откройте раздел **Пользователи** → **По API**
- Нажмите **Создать пользователя**
- Укажите название и описание(не обязательно) пользователя, выберите нужную роль (например, **SIGNER**, если он должен подписывать транзакции) и загрузите файл публичного ключа, созданный на шаге 1
- Нажмите **Сохранить**

После одобрения заявки новый API-пользователь появится в списке. Вы получите API Key (ID пользователя API) — уникальный идентификатор, который используется вместе с вашим секретным ключом.

Шаг 3: Получение авторизационного токена

```
# TODO
```

2.2 Авторизация
