Перелік методів API по роботі з порталом EDIN ID

> Всі запити нижче перерахованих API методів порталу EDIN ID направляються на адресу: https://id.edin.ua

> Для підписання хеш(ів) та/або файлу пароль передається в зашифрованому вигляді.

Авторизація

Кожен запит має містити HTTP header:

Header	Обов'язковий	Опис
`x-system-id`	так	Токен/ідентифікатор зовнішньої системи. Саме цей header використовується для авторизації.

Приклад:

```
curl -X GET 'https://host/api/external/company?...' \
  -H 'x-system-id: 019eb581-307b-7562-8a1f-20227511e898'
```

Сформувати Токен зовнішньої системи (x-system-id) може користувач з правами Суперадміністратора компанії на порталі EDIN ID.

Інструкція з формування Токена зовнішньої системи знаходиться за посиланням.

Отримання публічного ключа для шифрування паролів

Усі секретні значення, які передаються в API, мають бути зашифровані на актуальний публічний RSA-ключ сервера.

Це стосується таких полів:

Поле	Що передавати
Створити чернетку ключа: `info.caPassPhrase`	`base64(RSA-encrypt(publicKey, caPassPhraseBytes))`

Поле	Що передавати
Змінити статус співробітника: `adminKeyPassword`	`base64(RSA-encrypt(publicKey, adminKeyPasswordBytes))`
Перевірка ключа та пароля: requestbody.**password**	`base64(RSA-encrypt(publicKey, password))`
Підписати хеш ключем співробітника компанії: requestbody.**password**	`base64(RSA-encrypt(publicKey, password))`
Підписати файл ключем співробітника компанії: params.**password**	`base64(RSA-encrypt(publicKey, caPassPhraseBytes))`

API очікує саме **base64 від зашифрованих bytes**, а не plaintext пароль.

Інтеграція підписання в облікову систему

1	Отримати і зберегти публічний ключ	GET /api/external/key
2	Підписати хеш ключем співробітника компанії	POST /api/external/company/sign
3	Підписати файл ключем співробітника компанії	POST /api/external/company/sign/file
4	Верифікувати підпис на файлі	POST /api/external/company/sign/file/verify
5	Отримати інформацію про сертифікат	GET /api/external/company/key/certificate

> Колекція Postman

Інтеграція управління ключами в облікову систему

1	Отримати інформацію про компанію	GET /api/external/company
2	Отримати інформацію про співробітника	GET /api/external/company/employee
3	Пошук ключів співробітника	POST /api/external/company/employee/pkeys/search
4	Пошук співробітників компанії	POST /api/external/company/employees/search
5	Пошук ключів компанії	POST /api/external/company/pkeys/search
6	Отримати інформацію про ключ	GET /api/external/company/pkey
7.1	Отримати документ компанії	GET /api/external/company/form
7.2	Отримати ідентифікацію співробітника	GET /api/external/company/employee/identification
7.3	Отримати документ ключа	GET /api/external/company/pkey/form

8	Додати співробітника	POST /api/external/company/employee
9.1	Створити чернетку ключа	POST /api/external/company/employee/pkey/generate/draft
9.2	Згенерувати PDF-форму для адміністратора компанії	PATCH /api/external/company/employee/pkey/generate/draft
9.3	Передати підписи PDF і активувати ключ	POST /api/external/company/employee/pkey/activation
10	Змінити статус ключа	POST /api/external/company/pkey/status
11	Змінити статус співробітника	POST /api/external/company/employee/status
12	Створити компанію	POST /api/external/company/create
13	Перевірка ключа та пароля	PATCH /api/external/company/pkey

Створення ключа складається з трьох запитів:

1. Створити чернетку ключа та отримати PDF для підпису співробітником.
2. Згенерувати PDF для підпису адміністратором компанії.
3. Передати detached-підписи всіх PDF і активувати ключ або передати його на активацію КНЕДП.

Рекомендований сценарій створення та активації ключа:

1. Перевірити компанію методом 1.
2. Якщо співробітника ще немає – створити його методом 8.
3. Перевірити співробітника методом 2.
4. Викликати метод 9.1 і отримати `pKey.uuid` та employee PDF-форми.
5. Співробітник підписує PDF-форми з відповіді 9.1 detached-підписом.
6. Викликати метод 9.2 з `pKeyUuid` та `adminIpn` і отримати admin PDF-форми.
7. Адміністратор/суперадміністратор підписує PDF-форми з відповіді 9.2 detached-підписом.
8. Викликати метод 9.3, передавши `keyUuid`, `activate` і map підписів за всіма отриманими `formType`.
9. Отримати оновлений `ESSPrivateKey` зі статусом `ACTIVATED` або `COMPANY_ADMIN_APPROVED`.

Алгоритм підписання документа за допомогою КЕП EDIN ID

Алгоритм підписання документа за допомогою КЕП EDIN ID доступний за посиланням

Алгоритм підписання сертифіката за допомогою КЕП EDIN ID

Алгоритм підписання сертифіката за допомогою КЕП EDIN ID доступний за посиланням

Revision #29
Created 2026-04-22 16:30:57 UTC by Наталя Сідненко
Updated 2026-11-26 16:42:40 UTC by Наталя Сідненко