Методи API

Отримати і зберегти публічний ключ GET /api/external/key

REQUEST

URL	
Метод запиту	GET
URL запиту	**/api/external/key**
Authorization	
Auth type	API key
Key / Value	**x-system-id** / токен, отриманий при підключенні
Params	
type	тип відповіді JSON|PEM|XML (якщо параметр не передавати за замовченням буде JSON)

RESPONSE

В тілі **відповіді** повертається ключ у вказаному форматі:

- якщо type = JSON – повертається масив байт
- якщо type = PEM – повертається PEM-файл у вигляді

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQ9QIDAQAB
-----END PUBLIC KEY-----
```

- якщо type = XML – повертається XML-файл у вигляді

```
<?xml version="1.0"?>
<RSAKeyValue>
  <Modulus>wxWy8iReusbmiadsULVLSD36+l5k6cZ0=</Modulus>
  <Exponent>AQAB</Exponent>
</RSAKeyValue>
```

Для type in (PEM, XML) в reponse-header передається параметр `x-key-ttl`, в якому передається термін життя відкритого ключа.

Підписати хеш ключем співробітника компанії POST /api/external/company/sign

REQUEST

URL	
Метод запиту	POST
URL запиту	**/api/external/company/sign**
Authorization	
Auth type	API key
Key / Value	**x-system-id** / токен, отриманий при підключенні
Headers	
Content-Type	aplication/json

Request body	{
	"key": "{{id ключа}}",
	"password": "{{зашифрований пароль від ключа}}",
	"algorithm": "DSTU4145_GOST34311",
	"signType": "тип підпису, приймає значення CADES_BES, CADES_T, CADES_C, CADES_X_LONG, CADES_X_LONG_TRUSTED. Якщо не передано, за замовченням підставляється CADES_BES"
	"hashes": [
	{"hash": "{{хеш документа, що підписується}}", "description": "опис документа, що підписується"}
	]
	}

RESPONSE

В тілі **відповіді** повертається масив підписів.

Підписати файл ключем співробітника компанії POST /api/external/company/sign/file

REQUEST

URL	
Метод запиту	GET
URL запиту	**/api/external/company/sign/file**
Authorization	
Auth type	API key
Key / Value	**x-system-id** / токен, отриманий при підключенні
Headers	
Content-Type	multipart/form-data
Request body	Параметри тіла запиту: • **password** – зашифрований пароль. • **file.pdf** – дані (контент) для підпису у вигляді файлу або base64 (залежно від **inputFormat**)
Params	• **key** – ідентифікатор ключа. • **type –** тип підписання, може приймати значення: ◦ append – додає підпис до переданого файлу. **ВАЖЛИВО!** Якщо файл вже був підписаний, то підпис додається до існуючого, а не підписується разом з існуючим підписом. ◦ sign - підписує контент, використовується за замовчуванням. • **result –** формат підписання (дані й підпис в одному файлі, дані й підпис в окремих файлах), може приймати значення: ◦ enveloped – у відповідь надійде файл з підписом ◦ detached – у відповідь надійде тільки підпис • **inputFormat** – формат вхідних даних для підписання, може приймати значення: ◦ file – файл в бінарному вигляді

	◦ base64 – файл у вигляді base64 рядка • **outputFormat** – формат вихідних (результуючих) даних після підписання, може приймати значення: ◦ file – файл в бінарному вигляді ◦ base64 – файл у вигляді base64 рядка • **signType** – тип підпису, приймає значення CADES_BES, CADES_T, CADES_C, CADES_X_LONG, CADES_X_LONG_TRUSTED. Якщо не передано, то за замовченням підставляється CADES_BES

RESPONSE

В тілі **відповіді** повертається код 200 та результат підписання відповідно до параметрів **result** та **outputFormat.**