

## **Опис роботи сервісу BankID (взаємодія сервісу BankID з банком)**

Київ 2015

## Лист контролю версій

Версія	Дата	Опис
1.0	13.07.2015	Перша версія для загального обговорення
1.1	27.07.2015	Виправлення згідно зауважень НБУ

## Зміст

Зміст .....	3
Глосарій .....	4
1 Загальна частина .....	5
1.1 Призначення документа .....	5
1.2 Цілі створення сервісу .....	5
1.3 Концепція функціонування системи .....	5
2 Технічна архітектура системи .....	7
2.1 Процедура авторизації .....	8
2.1.1 Перехід на сторінку ІБ методом GET .....	8
2.1.2 Запит на отримання токenu доступу (access_token) методом POST .....	9
2.1.3 (Опціонально) Запит на продовження дії токenu (access_token) методом POST .....	10
2.2 Процедура отримання даних по клієнту .....	12
2.2.1 Запит даних по клієнту .....	13
2.2.2 Запит документів по клієнту .....	15

## Глосарій

Термін, скорочення	Визначення
<b>API</b>	Application Programming Interface. Набір готових класів, процедур, функцій, структур та констант, що надаються програмним комплексом (бібліотекою, сервісом) для використання у зовнішніх програмних продуктах.
<b>OAuth2.0</b>	Відкритий протокол авторизації, який дозволяє отримати третій стороні обмежений доступ до захищених ресурсів користувача без необхідності передавати їй (третій стороні) логін та пароль ( <a href="http://oauth.net/">http://oauth.net/</a> )
<b>ПАП</b>	Портал адміністративних послуг (або іноді Агент). Кінцева точка надання даних. Як правило мається на увазі сайт (портал) з надання адміністративних послуг в електронному вигляді.
<b>BankID</b>	Система для виконання верифікації користувача.
<b>JSON</b>	JavaScript Object Notation. Текстовий формат обміну даними, побудований на JavaScript.
<b>ІБ</b>	Веб-портал Інтернет Банкінгу. Система дистанційного обслуговування, яка працює в банку(у якій безпосередньо зареєстрований кінцевий користувач, що працює з ПАП).
<b>Авторизація</b>	Авторизація - керування рівнями та засобами доступу до певного захищеного ресурсу та ресурсів системи залежно від ідентифікатора і пароля користувача або надання певних повноважень.
<b>Автентифікація</b>	Автентифікація — процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора.

## 1 Загальна частина

### 1.1 Призначення документа

Опис функціональних вимог та процесу взаємодії сервісу BankID з банком.

### 1.2 Цілі створення сервісу

Забезпечення надійної та зручної верифікації користувача через його власний інтернет-банкінг на порталах адміністративних послуг.

### 1.3 Концепція функціонування системи

Для забезпечення масштабованості та гнучкості системи, передбачається, що на стороні банку (як правило на платформі існуючого у банку інтернет-банкінгу) буде реалізовано класичний OAuth2 сервер (згідно специфікації <http://tools.ietf.org/html/rfc6749>, рекомендовано використовувати готові рішення з сайту <http://oauth.net/2/> - секція *Server Libraries*, варіанти під усі популярні платформи та мови програмування). Сервіс BankID (як клієнтська сторона) проходить встановлену процедуру реєстрації, за результатом якої банк видає сервісу BankID параметри з'єднання (Client ID та Client Secret), та адресу для зворотного виклику (Redirect URI чи Callback URL). Інтеграція детально описана у [пункті 2](#) даного документу.

Функціонально система складається з трьох основних блоків:

1. **ПАП (веб-портал)**, на якому розміщені форми надання адміністративних послуг у електронному вигляді (замовлення довідок, внесення у реєстри тощо). При вході на портал та/або при замовленні конкретної послуги, користувачу доступна кнопка «авторизація через BankID».

Після натиснення кнопки «авторизація через BankID», користувач перенаправляється на сторінку вибору банку сервісу «Сервіс BankID».

В результаті успішного проходження процедури авторизації через BankID, користувач автоматично перенаправляється на сторінку порталу адміністративних послуг з підставленими даними електронної анкети.

2. **BankID (веб-сервер)**, на якому розміщена сторінка вибору банку та програмні процедури запиту/передачі даних з/до банку або порталу адміністративних послуг.

Після вибору користувачем банку, система перенаправляє його на сторінку логіна відповідного інтернет-банкінгу.

В результаті успішного проходження процедури логіну в інтернет-банкінг, інтернет-банкінг генерує код доступу до даних. За допомогою цього коду доступу «Сервіс BankID» робить автоматичний запит до інтернет-банкінгу для отримання електронної анкети та передає її до порталу адміністративних послуг.

Після вибору користувачем банку, система перенаправляє його на сторінку логіна відповідного інтернет-банкінгу. В результаті успішного проходження процедури логіну в інтернет-банкінг, інтернет-банкінг генерує код доступу до даних. За допомогою цього коду доступу «Сервіс BankID» робить автоматичний запит до інтернет-банкінгу для отримання персональних даних та передає їх до порталу адміністративних послуг.

3. **Банк (веб-портал інтернет-банкінгу або ІБ)**. У інтернет-банкінгу має бути реалізована сторінка логіну з призначенням коду доступу у разі успішної авторизації та програмні процедури отримання електронної анкети клієнта.

На сторінці логіну інтернет банкінгу користувач вводить логін пароль, разовий пароль з СМС або виконує інші дії передбачені конкретною системою інтернет-банкінгу. Далі користувач підтверджує перелік ресурсів до яких надає доступ (паспортні дані, сканкопії тощо). Після успішного логіну системою інтернет-банкінгу призначається код доступу до даних.

### Загальна схема функціонування сервісу BankID

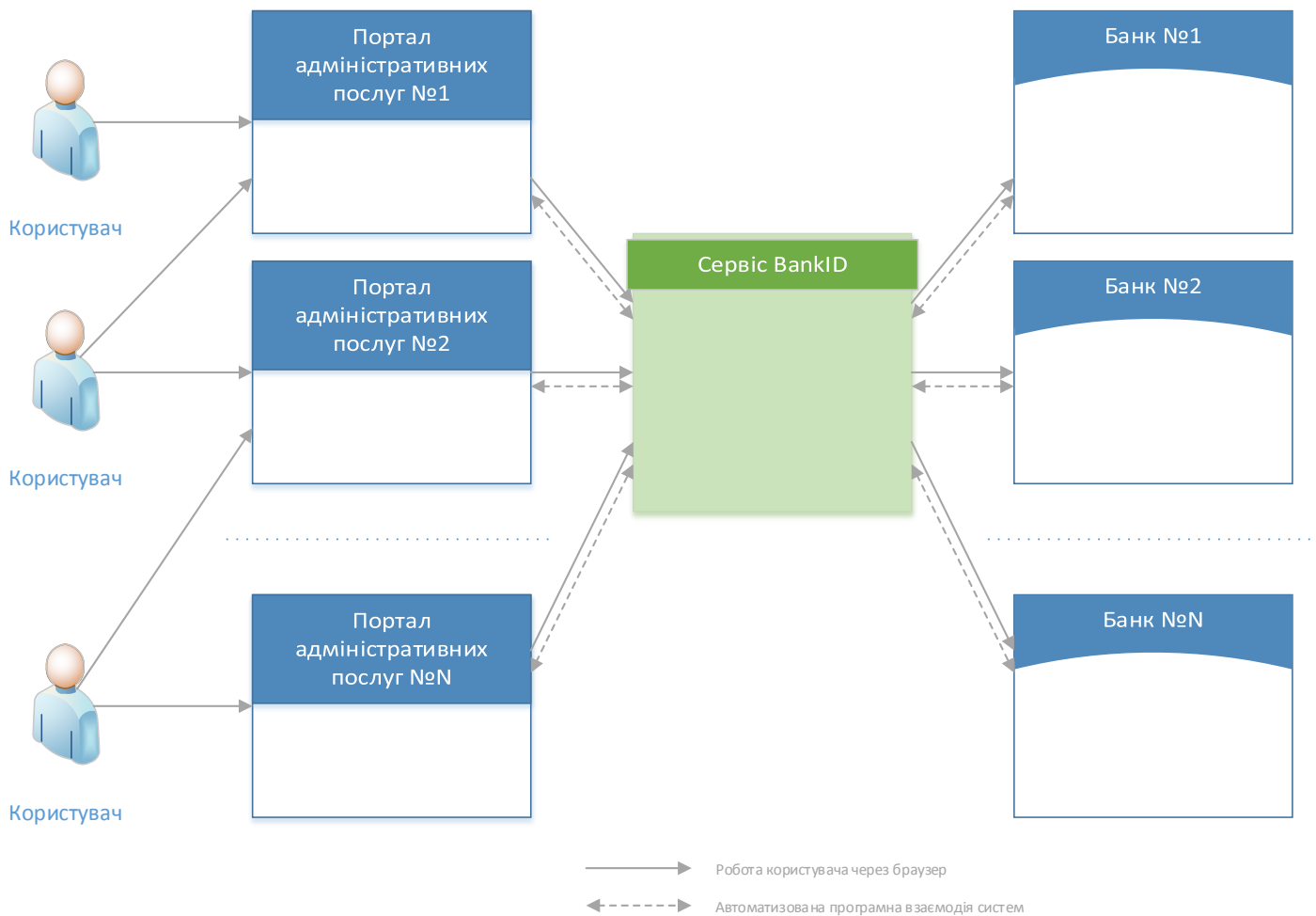


Рис. 1. Загальна схема функціонування сервісу BankID

## 2 Технічна архітектура системи

Взаємодія банку з сервісом BankID відбувається по стандартному протоколу OAuth2.0 згідно специфікації (<http://tools.ietf.org/html/rfc6749>).

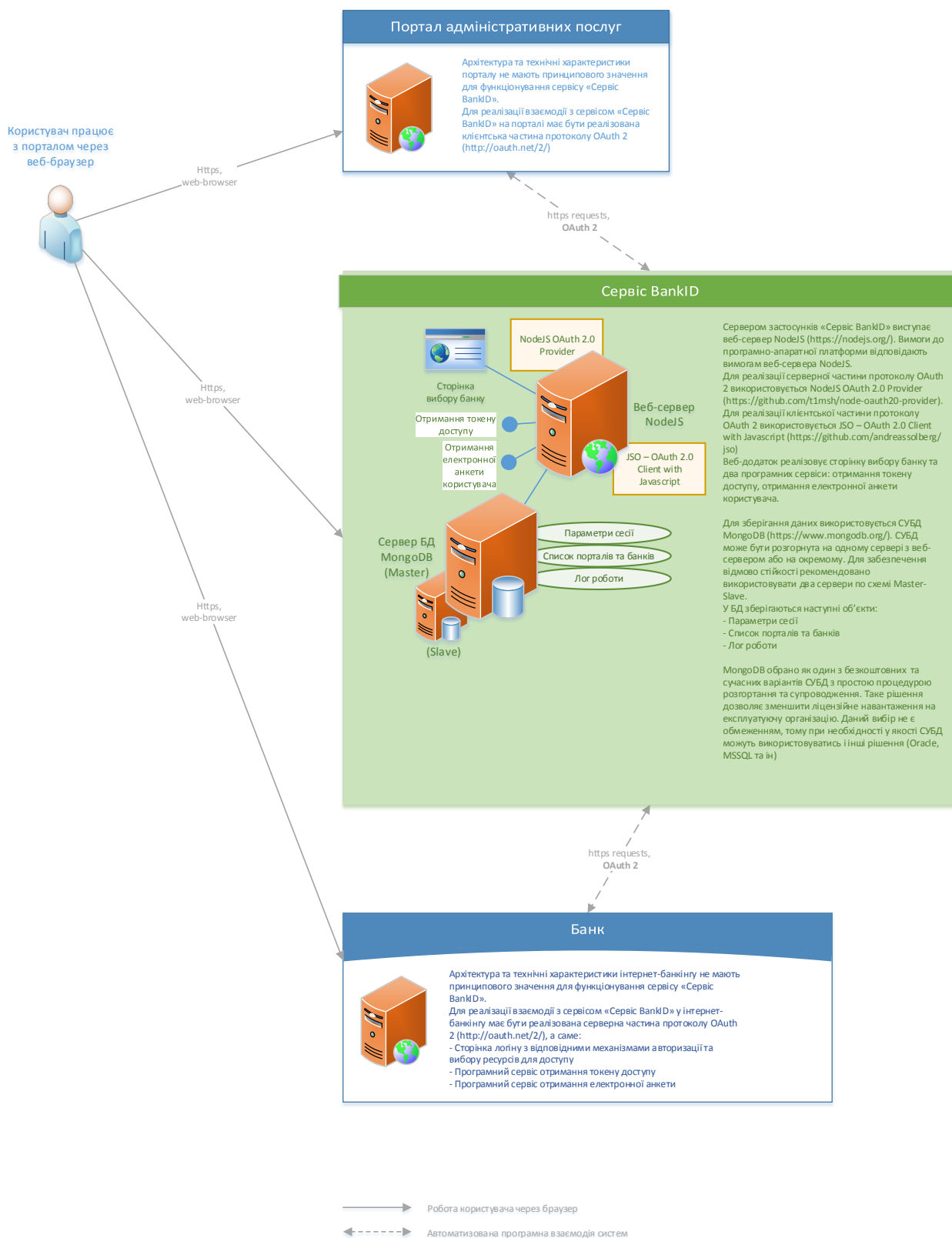


Рис. 2. Технологічна схема функціонування сервісу BankID

## 2.1 Процедура авторизації

### Документація API

Авторизація згідно стандарту OAuth 2.0 виконується у два етапи (Authorization Code Flow). Усі описані нижче методи повинні бути реалізовані на стороні ІБ банку.

#### 2.1.1 Перехід на сторінку ІБ методом GET

##### Запит

###### GET

```
/v1/bank/oauth2/authorize?response_type=code&client_id=client_id&redirect_uri=callback_url&state=state
```

HTTP/1.1

Параметр	Обов'язковість	Опис
client_id	Так	Унікальний ідентифікатор BankID у банку(видається банком для BankID при реєстрації одноразово)
callback_url	Так	Узгоджена заздалегідь адреса сайту BankID, на яку буде виконана переадресація з кодом (authorization code).Адреса фіксована, не повинна містити змінних параметрів (зміни у адресі повинні узгоджуватись зі стороною банку).
state	Ні, але бажано	Довільний параметр, який буде повернуто при переадресації на адресу, вказану у callback_url. Як правило використовується для уникнення <a href="#">CSRF</a> атак), бажане використання.

##### Відповідь

###### HTTP/1.1 200 OK

Переадресація на сторінку логіну у ІБ.

По завершенню авторизації користувача у своєму персональному ІБ буде виконано переадресацію на вказаній у параметрі **redirect\_url** користувача з поверненням параметру **code**

##### Помилки

Якщо при вказаному запиті виникають помилки, то можливі 2 ситуації:

- Клієнта (BankID) не вдалося автентифікувати (зокрема не зареєстрований на стороні банку) та невірно вказано адресу **callback\_url**. В такому випадку опис помилки повинен бути відображений у вікні ІБ.

- Клієнта (BankID) вдалося автентифікувати і переданий коректний **callback\_url**, проте сталася якась інша помилка – то буде виконано переадресацію на адресу **callback\_url** з наступними параметрами



Параметр	Обов'язковість	Опис
error	Так	Один з визначених кодів помилки. Повний перелік стандартних кодів можна знайти за посиланням <a href="https://tools.ietf.org/html/rfc6749#section-4.1.2.1">https://tools.ietf.org/html/rfc6749#section-4.1.2.1</a>
error_description	Ні	Текстовий опис помилки (у UTF-8 кодуванні), як правило деталізація для розробників.
error_uri	Ні	Адреса, за якою розміщено сторінку з детальним описом помилки, що сталася
state	Ні	Буде передано те ж значення, що використовувалось при початковому виклику (якщо було вказано).

## Приклад запиту

### Запит

```
GET https://vpn.unity-bars.com.ua:40103/Banking.Web/v1/bank/oauth2/authorize?response_type=code
&client_id=a18a1a63-7ace-434d-bd36-1538ad31d74d
&redirect_uri=https://bankid.unity-bars.com.ua:
40104/callback.htm&state=2364fc5d-c6b6-4f99-87a9-11d2baa32484
```

### Відповідь (переадресація з сайту ІБ)

```
GET https://bankid.unity-bars.com.ua:
40104/callback.htm?code=2d6f2318cb06cc2c97d948deb9799d608f1d5c97
&state=2364fc5d-c6b6-4f99-87a9-11d2baa32484
```

## 2.1.2 Запит на отримання токена доступу (access\_token) методом POST

### Запит

```
POST /v1/bank/oauth2/token HTTP/1.1
Content-Type: application/x-www-form-urlencoded

code=code
client_id=client_id&
client_secret=client_secret&
redirect_uri=callback_url&
grant_type=authorization_code
```

Параметр	Обов'язковість	Опис
code	Так	Код (authorization code), отриманий на попередньому кроці.
client_id	Так	Унікальний ідентифікатор BankID (видається банком при реєстрації одноразово)
client_secret	Так	Таємний код BankID(видається банком при реєстрації одноразово)
callback_url	Так	Узгоджена заздалегідь адреса сайту BankID, у даному випадку використовується

		для переадресації у разі виникнення помилок при отриманні токена доступу
--	--	--

**Відповідь**

HTTP/1.1 200 OK

Content-Type: application/json

```
{
  "token_type": "bearer",
  "access_token": "db8814c6d97cbad2a02db80e17d4676fab5914c6",
  "expires_in": 3600,
  "refresh_token": "91ee282ccda4e1af6dbd0da4920b206866278f5e"
}
```

**2.1.3 (Опціонально) Запит на продовження дії токена (access\_token) методом POST**

Для можливості продовжити дію вже отриманого токена (без необхідності виконання всіх попередніх викликів) необхідно виконати наступний запит

**Запит**

POST /v1/bank/oauth2/token HTTP/1.1

Content-Type: application/x-www-form-urlencoded

```
client_id=client_id&
client_secret=client_secret&
refresh_token=refresh_token&
grant_type=refresh_token
```

Параметр	Обов'язковість	Опис
client_id	Так	Унікальний ідентифікатор BankID (видається банком при реєстрації одноразово)
client_secret	Так	Таємний код BankID (видається банком при реєстрації одноразово)
refresh_token	Так	Значення токена (refresh_token), отриманого на кроці

**Відповідь**

HTTP/1.1 200 OK

Content-Type: application/json

```
{
  "token_type": "bearer",
  "access_token": "db8814c6d97cbad2a02db80e17d4676fab5914c6",
}
```

```
"expires_in":3600,  
}
```

## 2.2 Процедура отримання даних по клієнту

### Документація API

Отримання даних відбувається на основі токена доступу (access\_token), отриманого ході авторизації (згідно попереднього пункту). Токен необхідно передавати в заголовок запиту (headers) у вигляді:

Authorization: "Bearer access\_token"

Також сторона BankID в запиті повинна вказати, який саме набір полів по клієнту потрібно повернути після виклику. Опис усіх допустимих полів задається у вигляді JSON об'єкту:

```
{
  "type": "physical",
  "fields": ["firstName", "middleName", "lastName", "phone", "inn", "birthDay"],
  "scans": [
    { "type": "passport", "fields": ["link", "dateCreate", "extension"] },
    { "type": "zpassport", "fields": ["link", "dateCreate", "extension"] }
  ],
  "addresses": [
    { "type": "factual", "fields": ["country", "state", "area", "city", "street", "houseNo", "flatNo"] },
    { "type": "birth", "fields": ["country", "state", "area", "city", "street", "houseNo", "flatNo"] },
    { "type": "documents": [
      { "type": "passport", "fields": ["series", "number", "issue", "dateIssue", "dateExpiration", "issueCountryIso2"] },
      { "type": "zpassport", "fields": ["series", "number", "issue", "dateIssue", "dateExpiration", "issueCountryIso2"] }
    ]
  }
}
```

Тобто для отримання необхідних даних по клієнту потрібно передати підмножину вказаної структури (відсутність якогось з полів вказує на відсутність даних по цьому полю).

### Опис допустимих полів

Блок	Поле	Опис
fields	lastName	Прізвище
	firstName	Ім'я

	middleName	По батькові
	phone	Номер мобільного телефону
	inn	Ідентифікаційний код
	birthDay	Дата народження
	sex	Стать
	email	Електронна адреса
addresses	type	Тип адреси, допустимі значення <b>factual</b> і <b>birth</b> (фактична адреса та адреса народження відповідно)
	country	Країна
	state	Область
	area	Район
	city	Місто
	street	Вулиця
	houseNo	Номер будинку
	flatNo	Номер квартири
documents	type	Тип документу, допустимі значення <b>passport</b> , <b>zpassport</b> і <b>ident</b> (паспорт, закордонний паспорт, та посвідчення особи відповідно).
	typeName	Назва документу
	series	Серія документу
	number	Номер документу
	issue	Ким виданий документ
	dateIssue	Коли виданий
	dateExpiration	Термін дії
	issueCountryIso2	Країна видачі документу
scans	type	Копія документів, допустимі значення <b>passport</b> і <b>zpassport</b> (паспорт та закордонний паспорт відповідно)
	link	Посилання на файл копії для завантаження
	dateCreate	Дата створення документу
	extension	Розширення файлу

### 2.2.1 Запит даних по клієнту

#### Запит

**POST** /v1/bank/resource/client HTTP/1.1

Authorization: Bearer **access\_token**

Content-Type: application/json

{

```

"type": "physical",

"fields": ["firstName", "middleName", "lastName", "phone", "inn", "clId", "clIdText", "birthDay"],
"scans": [{"type": "passport", "fields": ["link", "dateCreate", "extension"]}],

"addresses": [{"type": "factual", "fields": ["country", "state", "area", "city", "street", "houseNo", "flatNo"]}],
"documents": [{"type": "passport", "fields": ["series", "number", "issue", "dateIssue", "dateExpiration", "issueCountryIso2"]}
]

```

Параметр	Обов'язковість	Опис
access_token	Так	Токен доступу, отриманий в процесі авторизації.

## Відповідь

HTTP/1.1 200 OK

Content-Type: application/json

```

{
  "state": "ok",
  "customer": {
    "type": "physical",
    "inn": "112233445566",
    "sex": "М",
    "email": "geraschenko@gmail.com.com",
    "birthDay": "20.01.1973",
    "firstName": "ПЕТРО",
    "lastName": "ГЕРАЩЕНКО",
    "middleName": "ІВАНОВИЧ",
    "phone": "+380961234511",
    "addresses": [
      {
        "type": "factual",
        "country": "UA",
        "state": "ВОЛИНСЬКА",
        "city": "Ківерці",
        "street": "Незалежності",
        "houseNo": "62",
        "flatNo": "12"
      }
    ],
    "documents": [
      {
        "type": "passport",
        "series": "AA",
        "number": "222333",
        "issue": "Ківерцівським РО УМВД",

```

```

        "dateIssue": "15.03.1999",
        "issueCountryIso2": "UA"
      },
    ],
    "scans": [
      {
        "type": "passport",
        "link": "https://vpn.unity-
bars.com.ua:40103/Banking.Web/v1/resource/client/scan/pasport",
        "dateCreate": "09.04.2015",
        "extension": "zip"
      }
    ]
  }
}

```

### 2.2.2 Запит документів по клієнту

Для отримання електронних файлів документів (сканованих копій) потрібно виконати запит методом **GET** за адресом, яку було повернуто у відповідному полі **link** блоку **scans** з загального блоку даних про клієнта, наприклад:

```

..
    "scans": [
      {
        "type": "passport",
        "link": "https://vpn.unity-
bars.com.ua:40103/Banking.Web/v1/resource/client/scan/pasport",
        "dateCreate": "09.04.2015",
        "extension": "zip"
      }
    ]
..

```

#### Запит

```

GET /v1/resource/client/scan/pasport HTTP/1.1
Authorization: Bearer access_token

```

#### Відповідь (файл на завантаження)

```

HTTP/1.1 200 OK
Content-Disposition:attachment; filename=passport.zip

```