

ЗАТВЕРДЖЕНО  
Рішення Ради Системи BankID  
Національного банку України  
(протокол 30.03.2021  
В/57-0007/24711)

**Специфікація взаємодії абонентського вузла  
абонента-надавача послуг з центральним вузлом  
Системи BankID Національного банку України**

## Аркуш контролю версій

Версія	Дата	Опис
1.0	13.07.2015	Перша версія для загального обговорення
1.1	27.07.2015	Виправлення зауважень, отриманих від НБУ
2.0	30.11.2015	Зміна версії
3.0	04.12.2015	Доповнення протоколу взаємодії Системи BankID НБУ – Банк: можливість взаємодії через сервіс-провайдера; передача даних анкети користувача в зашифрованому вигляді
3.1	10.03.2016	Виправлення URL (додавання /bank/)
3.2	13.10.2016	Додавання розділу щодо захисту інформації
3.3	31.10.2016	Унесені правки для узгодження тексту розділів із змістом розділу щодо захисту інформації
4	17.10.2018	Унесено правки та роз'яснення щодо порядку запитів у процесі взаємодії, доповнено види можливих помилок та роз'яснення щодо загального підходу шифрування/розшифрування даних. Доповнено перелік допустимих ключів для запиту персональних даних. Унесено виправлення для узгодження з новою редакцією Положення про Систему BankID Національного банку України. Зміна версії
4.1	23.06.2020	Окремі ключі електронної анкети визначені, як обов'язкові для заповнення. Доповнено вимоги, за яких електронне підтвердження дистанційної електронної ідентифікації вважається таким, що відповідає специфікації. Додано ключі memberId, uaResident, sidBi та можливість прямого запиту на банк через центральний вузол Системи BankID НБУ. Вилучено норму делегування банком функції ідентифікації користувача сервіс-провайдера. Внесено виправлення до ключів електронної анкети та прикладів. Додано уточнення по UTF-8 та опису контролю передачі даних. Внесено зміни у розділ щодо захисту інформації.
4.2.	30.03.2021	Ключ 'issueCountryIso2' вилучено із переліку ключів, обов'язкових для заповнення. Внесено уточнення щодо передачі даних по ключу 'documents'.

## ЗМІСТ

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.....	8
2.1. Процедура авторизації .....	9
2.1.1 Запит до центрального вузла Системи BankID НБУ методом GET (перший етап) .....	10
2.1.2 Запит на отримання коду доступу (access_token) методом POST (другий етап) .....	13
2.1.3 (Опціонально) Запит на продовження дії коду доступу (access_token) методом POST.....	15
2.2. Процедура отримання даних користувача.....	15
2.2.1. Електронна анкета (з переліком та описом допустимих ключів) .....	17
2.2.2. Запит даних користувача, як клієнта банку.....	21
3. Захист інформації в системі BankID НБУ.....	25
3.1. Загальні положення.....	25
3.2. Вимоги до використання криптографічного протоколу TLS та відповідних сертифікатів відкритих ключів .....	26
3.3. Вимоги до забезпечення конфіденційності та контролю цілісності електронної анкети.....	28

## Глосарій

№ зп	Термін, скорочення	Визначення
1	АБС	Автоматизована банківська система – автоматизована система банку – комплекс програмно-технічних засобів, спрямований на автоматизацію банківської діяльності. Забезпечує інтеграцію різних підсистем, кожна з яких спрямована на виконання тієї чи іншої сфери діяльності банку. У даному документі використовуються такі приклади підсистем АБС: ІБ (інтернет-банкінг).
2	Абонент Системи BankID НБУ	Абонент – надавач послуг або абонент-ідентифікатор.
3	Абонентський вузол Системи BankID НБУ	Комплекс програмно-технічних засобів, установлений в Абонента та призначений для забезпечення обміну інформацією між Абонентами через Систему BankID Національного банку.
4	Авторизація	Процес надання фізичній особі прав на виконання певних дій або доступу до ресурсів, а також процес перевірки (підтвердження) прав під час спроби виконання цих дій
5	Автентифікація	Процес перевірки достовірності. В Системі BankID НБУ це електронна процедура, що дає змогу підтвердити електронну дистанційну ідентифікацію фізичної особи.
6	ІБ	Інтернет-банкінг – технологія дистанційного банківського обслуговування, доступна користувачу за допомогою звичайного браузера з будь-якого комп'ютера, який має вихід в Інтернет.
7	Ідентифікація	Електронна дистанційна ідентифікація – процес розпізнавання фізичної особи абонентом – надавачем послуг із підтвердженням успішної автентифікації користувача Системи BankID Національного банку абонентом-ідентифікатором.
8	Кваліфікований сертифікат шифрування	Сертифікат відкритого ключа, виданий кваліфікованим надавачем довірчих послуг, який використовується в процесі обчислення узгодженого ключа шифрування ключів згідно з Вимогами до форматів криптографічних повідомлень (затверджені наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739).
9	ПП	Портал послуг – вебсайт (вебпортал), мобільний застосунок абонента – надавача послуг, на якому ініціюється електронний запит на електронну дистанційну ідентифікацію.

10	Система дистанційного обслуговування	Система надання банківських послуг користувачу без його безпосереднього звернення до відділення банку. Перед отриманням послуг користувач проходить попередню ідентифікацію та автентифікацію в системі за встановленою банком технологією.
11	Центральний вузол Системи BankID НБУ	Комплекс програмно-технічних засобів, що забезпечує взаємодію абонентських вузлів Абонентів Системи BankID Національного банку.
12	Система BankID НБУ	Національна система електронної дистанційної ідентифікації, яка виконує функції облікової і забезпечує здійснення електронної дистанційної ідентифікації фізичних осіб шляхом передавання персональних даних користувачів абонентом-ідентифікатором абоненту – надавачу послуг, а також здійснює облік кількості та обсягу наданих Абонентам послуг з електронної дистанційної ідентифікації.
13	OAuth	Відкритий протокол авторизації, який дає змогу третій стороні отримати обмежений доступ до захищених ресурсів користувача без необхідності передавати їй (третій стороні) логін та пароль ( <a href="http://oauth.net/">http://oauth.net/</a> ). У Системі BankID НБУ використовується протокол версії 2.0.

## 1. Загальна частина

### 1.1. Призначення документа

Опис функціональних вимог та процесу взаємодії абонентського вузла абонента-надавача послуг із центральним вузлом Системи BankID НБУ.

### 1.2. Цілі створення сервісу

Забезпечення на ПП надійної та зручної ідентифікації користувача через Систему BankID НБУ за участю банку (АБС), система якого передбачає ідентифікацію користувача як клієнта банку.

### 1.3. Концепція функціонування системи

Функціонально система складається з трьох основних блоків:

1. **ПП (вебсайт (вебпортал), мобільний застосунок)**, на якому розміщені форми надання послуг у електронному вигляді. Під час входу на портал або замовлення послуги користувачу доступна можливість авторизації

або ідентифікації за допомогою Системи BankID НБУ у вигляді банера або кнопки.

Після натискання кнопки або банера "авторизація/вхід/ідентифікація за допомогою Системи BankID НБУ" користувач із вебсторінки ПП може бути переадресований на вебсторінку банку одним із способів:

- через вебсторінку вибору банку на центрального вузла Системи BankID НБУ, на якій обирає банк, клієнтом якого він є, і переспрямовується на вебсторінку АБС відповідного банку для проведення процедури ідентифікації користувача;
- через пряме посилання, якщо у запиті від абонентського вузла абонента-надавача послуг передається параметр з ідентифікатором банку, наприклад, `&bank_id=oshadbank` (приклад в п.2.1.1).

Перелік ідентифікаторів для запиту з параметром банку доступний за посиланням - <https://id.bank.gov.ua/api/banks>.

На сторінці ПП користувач має бути ознайомлений з переліком даних що передаються і надати згоду на обробку персональних даних та шляхом проставлення відповідної позначки у явному вигляді.

У результаті успішного проходження процедури ідентифікації зі сторони АБС формується електронна анкета з персональними даними користувача (п. 2.2.), після чого користувач автоматично переадресовується назад на вебсторінку ПП. Одночасно ПП відповідно до порядку отримання даних отримує від АБС через Систему BankID НБУ підписану та зашифровану банком анкету з даними користувача.

**2. Центральний вузол Системи BankID НБУ**, на якому розміщена вебсторінка вибору банку та програмні процедури запиту/передачі даних між АБС та ПП на базі протоколу OAuth2.0.

Після вибору користувачем банку на вебсторінці центрального вузла Системи BankID НБУ користувач переадресовується на вебсторінку системи дистанційного обслуговування відповідного банку, на якій користувач як клієнт банку проходить стандартну процедуру ідентифікації та автентифікації (наприклад, вводить логін та пароль доступу до ІБ).

У результаті успішного проходження процедури ідентифікації та автентифікації користувача між АБС банку, центральним вузлом Системи BankID НБУ та ПП відбувається автоматична взаємодія отримання/передачі коду авторизації (**authorization\_code**), коду доступу (**access\_token**) та персональних даних.

**3. Банк (АБС: вебпортал інтернет-банкінгу або іншого сервісу банку)**, на вебсторінці якого, має бути реалізована форма ідентифікації користувача, програмні процедури автоматичного формування коду авторизації (**authorization\_code**), коду доступу (**access\_token**) та електронної анкети (п. 2.2.), накладення на неї кваліфікованої електронної печатки банку, шифрування даних анкети і переспрямування цієї анкети до ПП.

Користувач, перейшовши на вебсторінку АБС із заголовком “Ідентифікація через Систему BankID НБУ”, має можливість ідентифікуватися як клієнт обраного банку, наприклад, за допомогою номера картки банку або з використанням логіна та пароля, отриманих від банку. У разі успішної автентифікації користувач автоматично переспрямовується на сторінку ПП для продовження отримання послуги. Одночасно АБС банку повинна здійснити такі дії:

сформувати код авторизації (**authorization\_code**), за яким здійснюється запит на отримання коду доступу (**access\_token**),

сформувати код доступу, за яким буде здійснено запит необхідних персональних даних користувача (згідно з протоколом OAuth 2.0);

у відповідь на запит персональних даних перевірити відкритий ключ ПП, отриманий у кваліфікованому сертифікаті шифрування, та сформувати цифровий конверт із підписаними й зашифрованими персональними даними (формати підписаних та зашифрованих даних визначено Наказом Адміністрації ДССЗЗІ № 739 від 18.12.2012).

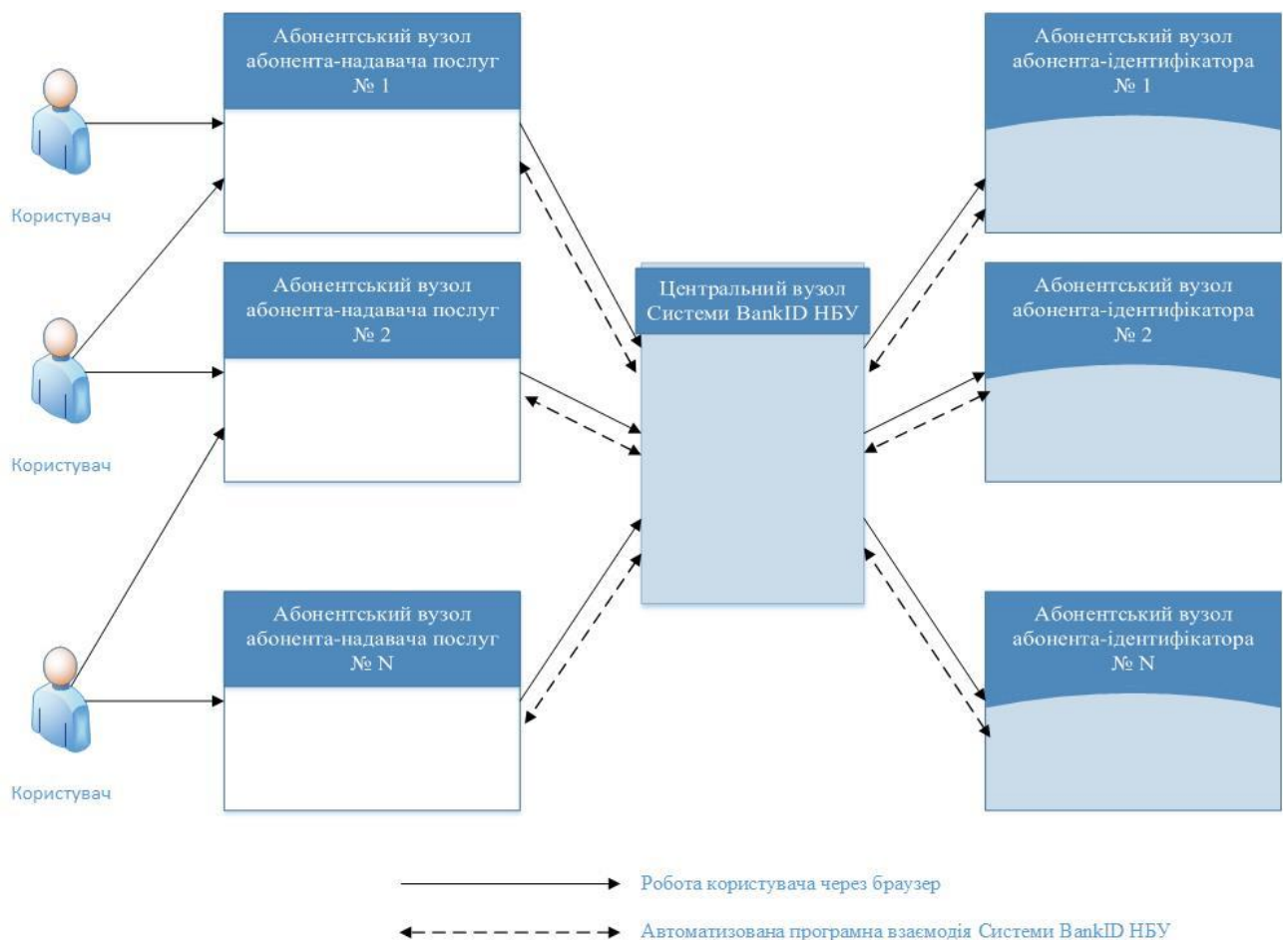


Рис. 1. Загальна схема функціонування Системи BankID НБУ

## 2. Технічна архітектура системи

Взаємодія ПП із центральним вузлом Системи BankID НБУ відбувається на базі протоколу OAuth2.0 згідно зі специфікацією, яка знаходиться за веб-адресою: <https://tools.ietf.org/html/rfc6749>. Рекомендовано використовувати готові рішення з вебсайту <http://oauth.net/2/> – секція “Code and Services”, варіанти під різні платформи та мови програмування.

Ідентифікація користувача відбувається засобами АБС відповідного банку. Дані, що передаються в відповіді АБС до ПП, шифруються симетричним ключем сеансу (ключ шифрування даних) за алгоритмом, визначеним у ДСТУ ГОСТ 28147-2009. В основі передачі даних лежить SSL-протокол.

Логіка роботи Системи BankID НБУ побудована на організації звернень від ПП до АБС конкретного банку через єдиний шлюз, яким виступає центральний вузол Системи BankID НБУ (далі – ц. в. BankID НБУ) та адресному передаванні необхідних даних від АБС банку до ПП у підписаному та зашифрованому вигляді. Усі абонентські вузли (як ПП, так і банків) взаємодіють виключно через ц. в. BankID НБУ.

Для підключення абонентського вузла абонента-надавача послуг до ц. в. Системи BankID НБУ уповноважена особа від абонента-надавача послуг надає DNS-адресу порталу послуг (**client\_host**), із якої будуть ініціюватись запити від абонентського вузла абонента-надавача послуг до ц. в. Системи BankID, та адресу для зворотного виклику (**callback\_url**). Адміністратор ц. в. Системи BankID НБУ видає цій уповноваженій особі унікальні ідентифікатори параметрів з'єднання (**client\_id**, **client\_secret**). Усі зазначені параметри є обов'язковими, мають бути фіксовані і не повинні містити змінних параметрів (зміни в адресах повинні узгоджуватися з головним адміністратором Системи BankID НБУ).

Параметр	Опис
<b>client_id</b>	Унікальний ідентифікатор ресурсу ПП, виду стрічки 32-шістнадцяткових значень, поділеної на групи дефісами. Надається адміністратором ц. в. BankID НБУ під час реєстрації, наприклад: 95e4ba81-06ad-4e97-b9d9-0728fbed074f
<b>client_secret</b>	Унікальний ідентифікатор секрету ресурсу ПП, виду стрічки 32-шістнадцяткових значень. Надається адміністратором ц. в. BankID НБУ під час реєстрації, наприклад: 5d42123a80942fda030c893c951fc08
<b>callback_url</b>	Веб-адреса ПП, на яку буде переадресовано користувача з ц. в. BankID НБУ у випадку проблем або помилок під час взаємодії.



	Надається стороною ПП під час реєстрації, наприклад: <a href="https://portal.example.com.ua/bankid/callback">https://portal.example.com.ua/bankid/callback</a>
<b>client_host</b>	Доменне ім'я ПП, із якого будуть ініціюватися запити до центрального вузла Системи BankID НБУ. Надається стороною ПП під час реєстрації, наприклад: <a href="https://portal.example.com.ua">https://portal.example.com.ua</a>

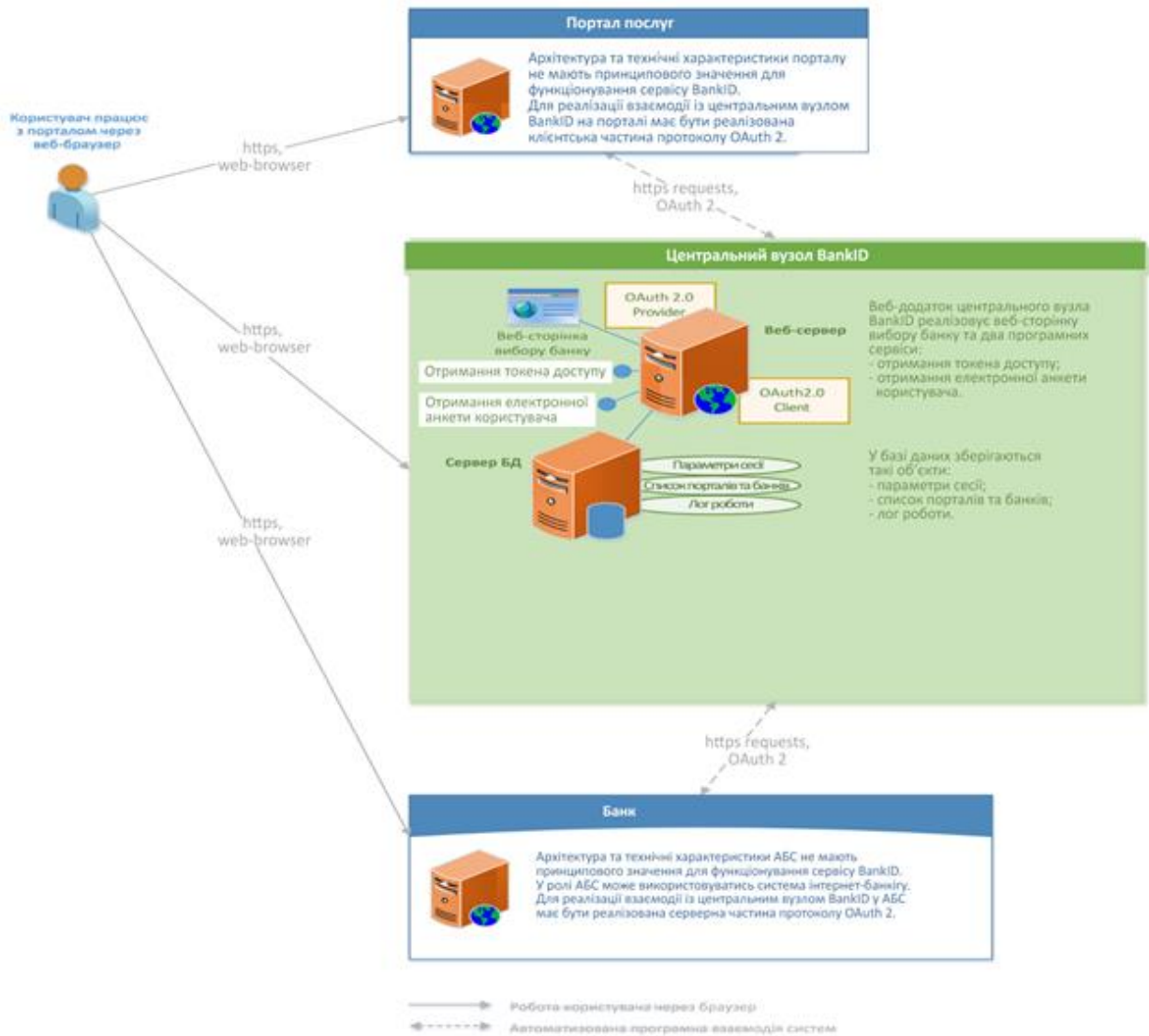


Рис. 2. Технологічна схема функціонування Системи BankID НБУ

## 2.1. Процедура авторизації

Авторизація згідно зі стандартом OAuth 2.0 виконується у два етапи:

перший етап – отримання коду авторизації (**authorization\_code**), параметр отриманий у запиті на веб адресу **callback\_url**, указану в запиті п. 2.1.1.1.;

другий етап – отримання коду доступу (**access\_token**) на підставі коду авторизації (запит на адресу ц. в BankID НБУ згідно з п.2.1.2.).

### 2.1.1 Запит до центрального вузла Системи BankID НБУ методом GET (перший етап)

Структура запиту від абонентського вузла абонента-надавача послуг до ц. в. BankID НБУ – запит формується під час переадресації користувача з кнопки “авторизація/вхід/ідентифікація за допомогою Системи BankID НБУ” на вебсторінці ПП у наступному форматі:

```
GET https://id.bank.gov.ua/v1/bank/oauth2/authorize?
  response_type=code&
  client_id=client_id&
  redirect_uri=callback_url&
  state=state&
  bank_id=bank_id
HTTP/1.1
```

Параметр	Опис
<b>callback_url</b>	Веб адреса ПП, на яку буде виконано запит із кодом авторизації ( <b>authorization_code</b> ) та переадресацію користувача. Адреса фіксована, не повинна містити змінних параметрів.
<b>state</b>	Довільний параметр, який буде повернуто в запиті з кодом авторизації на адресу порталу, вказану у <b>callback_url</b> . Бажане використання.
<b>bank_id</b>	Ідентифікатор банку за яким центральним вузлом здійснюється перенаправлення запиту порталу до конкретного банку. Перелік ідентифікаторів для запиту з параметром банку доступний за посиланням - <a href="https://id.bank.gov.ua/api/banks">https://id.bank.gov.ua/api/banks</a> . Параметр необов'язковий, використовується у випадках запиту до конкретного банку без переходу користувача на веб-сторінку ц.в. BankID НБУ.

Приклад запиту, за яким для вибору банку користувач перейде з вебсторінки ПП на вебсторінку ц. в. BankID НБУ:

```
GET https://id.bank.gov.ua/v1/bank/oauth2/authorize?
  response_type=code&
  client_id=a18a1a63-7ace-434d-bd36-1538ad31d74d&
  redirect_uri=https://portal.example.com.ua/callback.htm&
  state=2364fc5dc6b64f9987a911d2baa32484
```

Відповідь ц. в. BankID НБУ:

```
HTTP/1.1 200 OK
Перехід на вебсторінку ц. в. BankID НБУ, де користувач може обрати банк.
```

Приклад запиту, за яким користувача ц. в. BankID НБУ переадресує з вебсторінки ПП на вебсторінку ідентифікації користувача в банку:

```
GET https://id.bank.gov.ua/v1/bank/oauth2/authorize?
  response_type=code&
  client_id=a18a1a63-7ace-434d-bd36-1538ad31d74d&
  redirect_uri=https://portal.example.com.ua/callback.htm&
  state=2364fc5dc6b64f9987a911d2baa32484
  bank_id=oschadbank
```

Відповідь АБС банку:

```
HTTP/1.1 200 OK
Перехід на вебсторінку АБС банку для подальшої ідентифікації користувача в системі банку.
```

У разі успішної автентифікації користувача та отримання відповідного запиту від АБС банку ц. в. BankID НБУ повинен зробити запит із кодом авторизації **authorization\_code** на адресу параметра **redirect\_url**. Із даним запитом відбувається переадресація користувача до ПП.

Структура запиту з кодом авторизації від ц. в. BankID НБУ до ПП, у такому форматі:

```
GET https://portal.example.com.ua/v1/bank/oauth2/callback/code?
  code=authorization_code&
  state=state
HTTP/1.1
```

Параметр	Опис
<b>authorization_code</b>	Код авторизації — певний унікальний ідентифікатор який формується на стороні ц.в. BankID НБУ.
<b>state</b>	Буде вказано значення параметру яке передав ПП.

Приклад запиту до ПП:

```
GET https://portal.example.com.ua/v1/bank/oauth2/callback/code?
code=2d6f2318cb06cc2c97d948deb9799d608f1d5c97&
state=2364fc5dc6b64f9987a911d2baa32484
```

**Можливі помилки.**

Якщо на даному етапі виникають помилки, то можливі дві ситуації:

- ПП не вдалося автентифікувати (зокрема, ПП не зареєстрований на стороні ц. в. BankID НБУ або не співпадає значення певного параметра в запиті). У такому випадку опис помилки буде відображено на вебсторінці ц. в. BankID НБУ;

- користувача не вдалося автентифікувати на стороні АБС банку – буде виконано запит із переадресацією користувача на адресу значення **redirect\_url** із можливими значеннями помилок у параметрах запиту, наприклад:

```
GET https://portal.example.com.ua/v1/bank/oauth2/callback/code?
error=access_denied&
error_description=No_rights_for_BankID&
state=2364fc5dc6b64f9987a911d2baa32484
HTTP/1.1
```

Параметр	Опис
<b>error</b>	Один із визначених кодів помилки згідно зі специфікацією OAuth2.0 ( <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> ). Зокрема: <i>invalid_request</i> – у запиті відсутні обов’язкові значення або недопустимі значення певного параметра; <i>unauthorized_client</i> – неможливо отримати код авторизації; <i>access_denied</i> – запит заборонений.
<b>error_description</b>	Можливий текстовий опис помилки, деталізація для

	розробників
<b>state</b>	Буде вказано значення параметру яке передав ПП.

### 2.1.2 Запит на отримання коду доступу (**access\_token**) методом POST (другий етап)

Після отримання запиту з кодом авторизації ПП повинен ініціювати запит на отримання коду доступу. Структура запиту від ПП до ц. в. BankID НБУ під час якого значення передаються у вигляді стрічки з параметрами на вебадресу ц. в. BankID НБУ у такому форматі:

```
POST https://id.bank.gov.ua/v1/bank/oauth2/token HTTP/1.1
Content-Type: application/x-www-form-urlencoded
grant_type=authorization_code&
client_id=client_id&
client_secret=client_secret&
code=code&
redirect_uri=callback_url
```

Параметр	Опис
<b>grant_type</b>	Тип запиту, який повинен мати значення коду авторизації “ <b>authorization_code</b> ”, (в іншому випадку запит на продовження дії коду доступу ( <b>access_token</b> ) п.2.1.3. значення буде “ <b>refresh_token</b> ”)
<b>code</b>	Код авторизації ( <b>authorization code</b> ), отриманий від ц. в. BankID НБУ на попередньому кроці п.2.1.1.
<b>callback_url</b>	Адреса ПП, у даному випадку використовується для переадресації у разі виникнення помилок під час отримання коду доступу ( <b>access_token</b> )

У відповідь ц. в. BankID НБУ надає параметри та значення коду доступу в тілі запиту (*body*) у Json-форматі. Опціонально у відповіді параметр зі значенням **refresh\_token** не обов’язково передається. Використовується, коли термін дії коду доступу (**access\_token**) досить короткий і на ресурсі АБС банку реалізований цей функціонал.

Приклад відповіді ц. в. BankID:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
  "token_type": "bearer",
```

```

"access_token":"db8814c6d97cbad2a02db80e17d4676fab5914c6",
"expires_in":3600,
"refresh_token":"91ee282ccda4e1af6dbd0da4920b206866278f5e"
}

```

Параметр	Опис
<b>token_type</b>	Указується тип запиту під час якого передається код доступу, який повинен мати значення <b>"bearer"</b>
<b>access_token</b>	Значення коду доступу
<b>expires_in</b>	Термін дії коду доступу (значення в секундах)
<b>refresh_token</b>	Код оновлення запиту (опціонально, якщо підтримується АБС)

#### Можливі помилки.

У разі виникнення помилок оброблення запиту рекомендуємо орієнтуватися на список кодів стану HTTP. Також можуть передаватися параметри із значеннями помилки, що спричинили відмову, і передаються у тілі відповіді (*body*) у Json-форматі.

Приклад тіла відповіді з помилкою:

```

{"error":"invalid_grant", "error_description":"Invalid authorizathion code",
"code":"2d6f2318cb06cc2c97d948deb9799d608f1d5c97"}

```

Параметр	Опис
<b>error</b>	Один із визначених кодів помилки згідно специфікації <b>OAuth2.0</b> ( <a href="https://tools.ietf.org/html/rfc6749#section-5.2">https://tools.ietf.org/html/rfc6749#section-5.2</a> ). Наприклад: <b>invalid_request</b> - у запиті немає обов'язкових значень або неправильно сформованих значень одного або декількох параметрів; <b>invalid_grant</b> - некоректний код авторизації ( <i>authorization_code</i> ) або термін дії коду авторизації вичерпано.
<b>error_description</b>	Можливий текстовий опис помилки, деталізація для розробників
<b>code</b>	Буде вказано значення коду авторизації ( <i>authorization_code</i> ) при якому виникла помилка

### 2.1.3 (Опціонально) Запит на продовження дії коду доступу (`access_token`) методом POST

Якщо зі сторони АБС банку отримана відповідь зі значенням параметра `refresh_token`, то для можливості продовження дії вже отриманого коду доступу (без необхідності виконання всіх попередніх викликів) необхідно виконати такий запит:

структура запиту від ПП до ц. в. BankID НБУ – значення передаються у вигляді стрічки з параметрами на вказану веб адресу центрального вузла BankID НБУ в такому форматі:

```
POST https://id.bank.gov.ua/v1/bank/oauth2/token HTTP/1.1
Content-Type: application/x-www-form-urlencoded
grant_type=refresh_token&
client_id=client_id&
client_secret=client_secret&
refresh_token=refresh_token
```

Параметр	Опис
<code>grant_type</code>	Указується тип запиту, який на даному кроці повинен мати значення “ <code>refresh_token</code> ”
<code>refresh_token</code>	Значення токена ( <code>refresh_token</code> ), отриманого на попередньому кроці (п. 2.1.2)

У відповідь ц. в. BankID НБУ надає параметри та значення коду доступу в тілі запиту (*body*) в Json-форматі.

Приклад відповіді ц. в. BankID НБУ:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
  "token_type": "bearer",
  "access_token": "db8814c6d97cbad2a02db80e17d4676fab5914c6",
  "expires_in": 3600
}
```

## 2.2. Процедура отримання даних користувача

Отримання даних відбувається на підставі коду доступу (`access_token`), отриманого у ході авторизації (згідно з пунктом 2.1.2.). Код доступу необхідно передавати в заголовок запиту (`headers`) у вигляді:

Authorization: "Bearer **access\_token**"

Сторона ПП у запиті до ц. в. BankID НБУ повинна вказати, який саме набір даних щодо користувача, як клієнта банку, потрібно передати у відповіді, а також надати свій кваліфікований сертифікат шифрування закодований у BASE64. Ц. в. BankID НБУ переспрямовує отриманий запит на набір даних від ПП до АБС, у якому було здійснено автентифікацію користувача як клієнта банку.

Кваліфікований сертифікат шифрування передається в ключі "**cert**" закодований у BASE64. Порядок шифрування анкети визначено в пункті 3.3. цієї специфікації взаємодії.

Перелік необхідних даних вказується згідно з допустимими ключами у вигляді Json-об'єкту в тілі запиту (*body*). Якщо якийсь із ключів буде відсутнім або не визначено зі сторони АБС, то значення замовленого ключа не повертається або повертається зі значенням "null".

Приклад Json-об'єкта на запит персональних даних:

```
{
  "cert": "inThisValuePassOurCertificateEncodeToBase64Format==",
  "type": "physical",
  "fields": [
    "firstName", "middleName", "lastName", "phone", "inn", "birthDay", "sex",
    "flagPEPs", "flagPersonTerror", "flagRestriction", "flagTopLevelRisk"
  ],
  "addresses": [
    { "type": "factual", "fields": [
      "country", "state", "area", "city", "street", "houseNo", "flatNo"
    ] },
    { "type": "juridical", "fields": [
      "country", "state", "area", "city", "street", "houseNo", "flatNo"
    ] }
  ],
  "documents": [
    { "type": "passport", "fields": [
      "series", "number", "issue", "dateIssue", "dateExpiration", "issueCountryIso2"
    ] },
    { "type": "zpassport", "fields": [
      "series", "number", "issue", "dateIssue", "dateExpiration", "issueCountryIso2"
    ] }
  ]
}
```



```

"scans":[
  {"type":"passport","fields":["scanFile","dateCreate","extension"]},
  {"type":"zpassport","fields":["scanFile","dateCreate","extension"]}
]
}

```

Тобто для отримання необхідних даних про користувача потрібно передати всі ключі, які необхідні. Відсутність ключа вказує на те, що такі дані передавати не потрібно.

### 2.2.1. Електронна анкета (з переліком та описом допустимих ключів)

Ключ			Значення ** (формат та вимоги)	Опис
1	2	3	4	5
<b>cert*</b>			Закодовано по стандарту BASE64.	Кваліфікований сертифікат шифрування
<b>memberId</b>			XXXXXXXXNN – де: XXXXXXXX – ідентифікатор абонента (код ЄДРПОУ); NN – порядковий номер абонентського вузла. Ключ та значення "memberId" додаються ц. в. BankID НБУ.	Унікальний ідентифікатор вузла абонента в Системі BankID НБУ
<b>sidBi</b>			Ключ та значення додаються ц. в. BankID НБУ.	Ідентифікатор сесії
<b>type</b>			physical	Значення ідентифікації фізичної особи. На даний час приймає тільки одне значення – physical.
	<b>fields</b>	<b>Масив з даними по особі</b>		
		lastName*		Прізвище
		firstName*		Ім'я
		middleName*		По батькові
		phone	380XXXXXXXXX - де X може приймати тільки цифрове значення.	Номер телефону
		inn*	Заповнюється відповідно до вимог законодавства України	Реєстраційний номер облікової картки платника податків, номер (та за наявності - серію) паспорта громадянина України, в якому проставлено відмітку про відмову від прийняття реєстраційного номера облікової картки платника податків, чи номер паспорта із записом про відмову від прийняття реєстраційного номера облікової картки платника податків в електронному безконтактному носії.
		clientId		Унікальний ідентифікатор клієнта в банку.

Ключ		Значення ** (формат та вимоги)		Опис
1	2	3	4	5
				У випадку якщо банк не має такого ідентифікатора, можливо вказати значення ключа inn або серію й номер паспорта.
		clIdText	“Інформація надана засобами Системи BankID НБУ dd.mm.yyyy hh.mm”	Статичний текст з інформацією про надані дані банком щодо користувача, дата і час надання
		birthDay*	dd.mm.yyyy	Дата народження.
		sex*	Можливі значення: латинська літера M – чоловіча або F – жіноча	Стать
		email		Електронна адреса
		socStatus	Наприклад: “студент”, “пенсіонер”, “тимчасово безробітний”, “працюючий”, “нерегулярна зайнятість”.	Соціальний статус
		flagPEPs	Можливі значення: 1 – так, 0 – ні.	Ознака, чи визначена фізична особа банком-повіреною такою, що належить до категорії PEPs (публічні особи, близькі, пов’язані).
		flagPersonTerror	Можливі значення: 1 – так, 0 – ні.	Ознака, чи визначена фізична особа банком-повіреною такою, що включена до переліку осіб, пов’язаних зі здійсненням терористичної діяльності або щодо яких застосовано міжнародні санкції.
		flagRestriction	Можливі значення: 1 – так, 0 – ні.	Ознака, чи визначена фізична особа банком-повіреною такою, що включена до переліку осіб, щодо яких застосовані персональні, спеціальні економічні та інші обмежувальні заходи (санкції), санкції РНБОУ.
		flagTopLevelRisk	Можливі значення: 1 – так, 0 – ні.	Ознака, чи присвоєний клієнту банком-повіреною (неприйнятно) високий рівень ризику ПВК/ФТ.
		uaResident	Можливі значення: 1 – так, 0 – ні.	Ознака, чи визначена фізична особа банком-повіреною такою, що є резидентом України.
<b>addresses</b>	<b>Масив типів адрес та адресних даних особи</b>			
	type*		Можливі значення: <b>factual,</b> <b>juridical.</b>	Тип адреси проживання: <b>factual</b> – фактична адреса проживання, <b>juridical</b> - адреса реєстрації.
	<b>fields</b>	<b>Масив адресних даних особи</b>		
		country*	Двозначний літерний код країни за стандартом ISO_3166-1 (alfa-2). Наприклад: UA	Країна
		state*		Область. Якщо адреса користувача не передбачає наявності області, відповідне значення не передається у відповіді абонента-

Ключ			Значення ** (формат та вимоги)	Опис
1	2	3	4	5
				ідентифікатора.
		area*		Район. Якщо адреса користувача не передбачає наявності району, відповідне значення не передається у відповіді абонента-ідентифікатора.
		city*		Місто
		street*		Вулиця
		houseNo*		Номер будинку
		flatNo*		Номер квартири. Якщо адреса користувача не передбачає наявності номеру квартири, відповідне значення не передається у відповіді абонента-ідентифікатора.
<b>documents</b>	<b>Масив типів документів та реквізити документів що засвідчують особу</b>			
	type*		Можливі значення: <b>passport,</b> <b>idpassport,</b> <b>zpassport,</b> <b>ident.</b>	Тип документу: <b>passport</b> – паспорт; <b>idpassport</b> – id-картка; <b>zpassport</b> – закордонний паспорт; <b>ident</b> – посвідчення особи у відповідності до вимог законодавства України.
	<b>fields</b>	<b>Масив реквізитів документів що засвідчують особу</b>		
		typeName*		Назва документу
		series*		Серія документа (для типу <b>idpassport</b> - не заповнюється).
		number*		Номер документа
		issue*		Яким органом видано документ
		dateIssue*	dd.mm.yyyy	Дата видачі документа
		dateExpiration*	dd.mm.yyyy	Термін дії (для типу <b>passport</b> - не заповнюється)
		issueCountryIso2	Двозначний літерний код країни за стандартом ISO_3166-1 (alfa-2). Наприклад: UA	Країна видачі документа
<b>scans</b>	<b>Масив скан-копій з типами та файлами документів особи</b>			
	type		Можливі значення: <b>passport,</b> <b>idpassport,</b> <b>zpassport,</b> <b>inn,</b> <b>personalPhoto.</b>	Тип відсканованого документа: <b>passport</b> – паспорт; <b>idpassport</b> – id-картка; <b>zpassport</b> – закордонний паспорт; <b>inn</b> – реєстраційний номер облікової картки платника податків; <b>personalPhoto</b> – фото особи (анфас).
	<b>fields</b>	<b>Масив з файлів скан-копій</b>		
		scanFile	Закодований по стандарту BASE64. Якщо скан-копія знаходиться в архіві, то файл скан-копій	Файл сканованої копії документа. Рекомендована роздільна здатність скан-копії не менше 200 DPI.

Ключ		Значення ** (формат та вимоги)		Опис
1	2	3	4	5
			обов'язково повинен мати розширення (наприклад: pdf, jpg, png, bmp).	
	dateCreate		dd.mm.yyyy	Дата створення скан-копії документа
	extension		У випадку, якщо файли об'єднанні або заархівовані у zip форматі, то зазначається розширення zip.	Розширення файлу, який знаходиться в значенні ключа scanFile.

\* - обов'язкові ключі для заповнення абонентом-ідентифікатором.

\*\* - всі значення ключів мають символічний тип.

Дані клієнта, передані через ц. в. Системи BankID НБУ у відповіді від АБС вважаються такими, що відповідають вимогам цієї специфікації у випадку виконання наступних вимог.

Банк зобов'язаний передати дані клієнта за ключами, що позначені у цій анкеті, як обов'язкові до заповнення та містяться у запиті абонента-надавача послуг. У разі невиконання цієї умови банком, електронне підтвердження електронної дистанційної ідентифікації вважається таким, що не відповідає специфікації взаємодії та не підлягає тарифікації за міжабонентськими тарифами.

Дані клієнта за ключами, які не позначені у цій специфікації як обов'язкові до заповнення, не підлягають обов'язковій передачі банком, а відсутність такої інформації у відповіді АБС не є підставою для не здійснення тарифікації електронного підтвердження електронної дистанційної ідентифікації.

За запитом абонента-надавача послуг на отримання даних клієнта за двома або більше документами (ключ "documents"), банк зобов'язаний передати дані по клієнту не менше ніж за одним із **запитуваних** документів: паспорт громадянина України ("passport"), id-картка ("idpassport"), паспорт громадянина України для виїзду за кордон ("zpassport"), посвідчення особи у відповідності до вимог законодавства України ("ident"). За виконання цієї умови, інформація надана у відповіді АБС за одним із значень (документів) ключа "documents" є такою, що надана у повному обсязі відповідно до вимог специфікації взаємодії.

У разі запиту абонента-надавача послуг на отримання даних клієнта:

за документом паспорт громадянина України ("passport") ключ "dateExpiration" не є обов'язковим до заповнення;

за документом id-картка ("idpassport") ключ "series" не є обов'язковим до заповнення.

Значення ключа "scans" заповнюється абонентом-ідентифікатором виключно на запит банків, зареєстрованих у Системі BankID НБУ у статусі абонентів-надавачів послуг та може бути використана такими абонентами –

надавачами послуг виключно для надання фінансових послуг без права передавання її третім особам.

### 2.2.2. Запит даних користувача, як клієнта банку

Для отримання даних щодо користувача направляється запит від ПП до ц. в. BankID НБУ. Параметри та значення передаються в тілі запиту (*body*) в Json-форматі.

Приклад запиту щодо даних від ПП:

```
POST https://id.bank.gov.ua/v1/bank/resource/client HTTP/1.1
Authorization: Bearer access_token
Content-Type: application/json
{
  "cert": "dEBIGx1pdL6dt1ngaOEFvt/ik9eUpDuz90rm/Vk23v+FtiKJEvGnu
ea9FGjvBMGIFZS4zhg2IYIHGOhlBVYrZcez6udotjZlCLGZ7zwPuFo0XypKDQ
j5qpR7w0rFFZNjcPH3JW2IzEUv.....",
  "type": "physical",
  "fields": [
    "firstName", "middleName", "lastName",
    "phone", "inn", "cId", "cIdText", "birthDay", "sex"
  ],
  "addresses": [
    { "type": "factual", "fields": [
      "country", "state", "area", "city", "street", "houseNo", "flatNo"
    ]
  },
  "documents": [
    { "type": "passport", "fields": [
      "series", "number", "issue",
      "dateIssue", "dateExpiration", "issueCountryIso2"
    ]
  },
  "scans": [
    { "type": "passport", "fields": [
      "scanFile", "dateCreate", "extension"
    ]
  }
}
```

Параметр	Опис
<b>access_token</b>	Код доступу, отриманий у відповіді від ц. в. BankID НБУ

Відповідь надається у вигляді Json-об'єкта, в якому банк передає через ц. в. BankID НБУ свій кваліфікований сертифікат шифрування та цифровий конверт, що містить зашифровані й підписані персональні дані. Кваліфікований сертифікат шифрування банку міститься в у значенні ключа "**cert**" закодований у BASE64. Цифровий конверт із даними про користувача в підписаному та зашифрованому вигляді разом із зашифрованим ключем шифрування даних містяться в у значенні ключа "**customerCrypto**" закодований у BASE64.

Приклад відповіді:

```

HTTP/1.1 200 OK
Content-Type: application/json
{
  "state": "ok",
  "cert": "dEBIGx1pdL6dt1ngaOefPvt/ik9eUpDuz90rm/Vk23v+FtiKJEvGnu
ea9FGjvBMGI FZS4zhg2IYIHGOhlBVYrZcez6udotjZlCLGZ7zwPuFo0XypKDQ
j5qpR7w0rFFZNjcPH3JW2IzEUv.....",
  "customerCrypto":
  "dEBIGx1pdL6dt1ngaOefPvt/ik9eUpDuz90rm/Vk23v+FtiKJEvGnuea9FGjvBM
GIFZS4zhg2IYIHGOhlBVYrZcez6udotjZlCLGZ7zwPuFo0XypKDQj5qpR7w0rF
FZNjcPH3JW2IzEUv/4bXQWqYCccma03b3lbva+YJ/Txox1CMfyV4jJ5fXeCMO
jEWxwctEc7mXNzPfcBKMoqr048uvW9HTiPkjsLIU5jgTKJVdgoanZI4712dmQe
v5UzMKqNYvOwfJ+hU872kCSD1wfgVaJU0qP6yURcK80ys2K5OvUpa9uIHw
mL7KmnxMDhB4hLr5CQP11XZ09RnNykgS/4cQ.....",
  "memberId": "9999999901",
  "sidBi": "2baeadd0-c7e6-4ad9-9181-1fd9bbebfaac"
}

```

Розшифрування підписаних персональних даних користувача відбувається згідно з вимогами до форматів криптографічних повідомлень, визначених наказом Адміністрації Державної служби спеціального зв'язку та захисту

інформації України від 18.12.2012 № 739 (<http://zakon3.rada.gov.ua/laws/show/z0108-13>) (далі – Вимоги). Узгодження ключів за замовчуванням здійснюється з використанням статичного механізму. Якщо параметри криптографічного алгоритму статичної ключової пари відправника не еквівалентні параметрам криптографічного алгоритму статичної ключової пари одержувача, повинен здійснюватися перехід до застосування динамічного механізму узгодження ключів. Засоби криптографічного захисту інформації відправника та одержувача мають підтримувати криптографічні алгоритми, визначені цими Вимогами.

АБС банку формує Json-об'єкт у стандарті кодування UTF-8 із персональними даними користувача у вигляді (приклад):

```
{
  "type":"physical",
  "inn":"112233445566",
  "sex":"М",
  "email":"geraschenko@gmail.com",
  "birthDay":"20.01.1953",
  "firstName":"ПЕТРО",
  "lastName":"ГЕРАЩЕНКО",
  "middleName":"ІВАНОВИЧ",
  "phone":"380961234511",
  "clId":"6299E05EC5D568733C14CCEF9C975DD3",
  "clIdText":"Інформація надана засобами Системи BankID НБУ 25.12.2017
19:40",
  "socStatus": "пенсіонер",
  "flagPEPs":"0",
  "flagPersonTerror":"1",
  "flagRestriction":"0",
  "flagTopLevelRisk":"1",
  "uaResident":"1",
  "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",
    "scanFile":"H4sIAAAAAAAAAEAOS8dVhczZYuHtxdQiBA4wRraNwdg
ru7NO7uFpwEd3cLwTEd3cLwEd3cLwEd3cLwEd3cLwEd3cLwE.....",
    "dateCreate":"09.04.2015",
```

```

    "extension": "zip"
  }}
}

```

Після цього вказаний Json-об'єкт підписується кваліфікованою електронною печаткою банку й шифрується симетричним ключем сеансу (КШД – ключ шифрування даних за алгоритмом, визначеним у ДСТУ ГОСТ 28147-2009). Підписаний та зашифрований об'єкт формується у вигляді цифрового конверта згідно з Вимогами.

Примітка. Сам ключ шифрування даних шифрується узгодженим ключем (КШК – ключ шифрування ключа, симетричний ключ, який обчислюється за протоколом Діффі-Геллмана на підставі пари ключів – відкритого ключа шифрування ПП, отриманого з кваліфікованого сертифіката ПП, та особистого ключа шифрування АБС банку).

#### Можливі помилки.

У разі виникнення помилок оброблення запиту рекомендуємо орієнтуватися на список кодів стану HTTP. Якщо стан запиту дорівнює 200, то необхідно перевіряти тіло запиту (логічна помилка), в іншому випадку – це технічна помилка. Параметри зі значеннями помилки передаються в тілі запиту (*body*) у Json-форматі.

#### Приклад технічної помилки:

```

{"error": "invalid_token", "error_description": "Invalid access_token",
"access_token": "db8814c6d97cbad2a02db80e17d4676fab5914c6"}

```

#### Приклад логічної помилки:

```

{"error": "invalid_cert", "error_description": "Sertificate not found at
EUSignCP.EUPackHelper.EnvelopData(Byte[] data)", "code": "CL003",
"memberId": "9999999901", "sidBi": "2baeadd0-c7e6-4ad9-9181-1fd9bbebfaac"}

```

Параметр	Опис
<b>error</b>	<p>Приклади технічних помилок:</p> <p><b>invalid_request</b> – у запиті немає обов'язкових або неправильно сформованих значень;</p> <p><b>invalid_token</b> – некоректний код доступу (<b>access_token</b>) або термін дії коду доступу вичерпано.</p> <p>Приклад логічних помилок:</p>



	<b>invalid_cert</b> – проблеми під час оброблення кваліфікованого сертифікату, зокрема некоректний/недійсний сертифікат або проблеми з підписом; <b>invalid_data</b> – ключі в запиті щодо користувача некоректні.
<b>error_description</b>	Текстовий опис помилки, деталізація для розробників
<b>code</b>	Певне значення, яке може допомогти банку для аналізу причини помилки.

### 3. Захист інформації в Системі BankID НБУ

#### 3.1. Загальні положення

Передавання інформації між абонентами Системи BankID НБУ має здійснюватися із забезпеченням конфіденційності та контролю цілісності.

Абонентські вузли та ц. в. Системи BankID НБУ забезпечують ідентифікацію й автентифікацію у своїх інформаційно-телекомунікаційних системах із використанням криптографічного протоколу TLS (Transport Layer Security), вимоги до якого наведено нижче.

У системах абонентів-надавачів послуг, абонентів-ідентифікаторів (банків), центрального вузла Системи BankID НБУ здійснюється реєстрація подій шляхом ведення журналу аудиту.

Журнал аудиту абонентського вузла абонента-надавача послуг повинен містити відомості про факт відправлення електронного запиту на ідентифікацію до центрального вузла Системи BankID НБУ, отримання електронного підтвердження ідентифікації від центрального вузла Системи BankID НБУ, результат розшифрування електронного підтвердження ідентифікації, результат перевірки кваліфікованого електронного підпису/печатки, накладеного абонентом-ідентифікатором(банком).

Журнал аудиту абонента-ідентифікатора (банку) повинен містити відомості про факт звернення користувача Системи BankID НБУ, результат опрацювання звернення користувача Системи BankID НБУ, факт відправлення електронного підтвердження ідентифікації центральному вузлу Системи BankID НБУ.

Журнал аудиту центрального вузла Системи BankID НБУ повинен містити відомості про факт проходження електронного запиту на ідентифікацію від абонента-надавача послуг через центральний вузол Системи BankID НБУ до абонента-ідентифікатора та про факт проходження електронного

підтвердження ідентифікації від абонента-ідентифікатора через центральний вузол Системи BankID НБУ до абонента-надавача послуг.

Абоненти – надавачі послуг, абоненти-ідентифікатори, адміністратори абонентських вузлів, адміністратор центрального вузла Системи BankID НБУ мають право самостійно визначати додаткові події, що фіксуються у відповідних журналах аудиту.

Усі записи в журналах аудиту повинні містити опис події, дату та час події, а також забезпечувати ідентифікацію суб'єкта, який ініціював подію.

Журнали аудиту повинні мати захист від несанкціонованого доступу, модифікації та знищення (руйнування).

Взаємодія центрального вузла Системи BankID НБУ з системами абонентів-надавачів послуг та абонентів-ідентифікаторів здійснюється виключно з використанням параметрів та адрес, які узгоджені із адміністратором центрального вузла Системи BankID НБУ.

З метою контролю передачі даних на зареєстровані вебсайти, програмним забезпеченням центрального вузла Системи BankID НБУ, виконується перевірка вебадреси параметру запиту **redirect\_uri** з вебадресою зареєстровану за цим ПП по полю **clientHost**, відповідно до ідентифікатора ПП (по параметру **client\_id**).

Наприклад:

а) якщо зареєстровано **clientHost=https://example.com.ua**:

- ідентифікацію буде дозволено, якщо запит з параметрами  
**redirect\_uri = https://example.com.ua**  
**redirect\_uri = https://example1.example.com.ua**
- ідентифікацію не буде дозволено, якщо запит з параметром  
**redirect\_uri = https://exammmmples.com.ua**

б) якщо зареєстровано **clientHost = https://example1.example.com.ua**

- ідентифікацію буде дозволено, якщо запит з параметрами  
**redirect\_uri = https://example1.example.com.ua**
- ідентифікацію не буде дозволено, якщо запит з параметром  
**redirect\_uri = https://example.com.ua**  
**redirect\_uri = https://example2.example.com.ua**

У випадку заблокованої ідентифікації користувачеві відобразатиметься повідомлення з інформацією про невідповідність зареєстрованої вебадреси до параметра запиту.

### 3.2. Вимоги до використання криптографічного протоколу TLS та відповідних сертифікатів відкритих ключів

Абонентські вузли та ц. в. Системи BankID НБУ для встановлення безпечного з'єднання між собою та з користувачами Системи BankID НБУ

повинні використовувати криптографічний протокол TLS не нижче версії 1.2, а також відповідні особисті ключі та сертифікати відкритих ключів.

У протоколі TLS допускаються різні криптографічні набори.

Криптографічний набір узгоджується між клієнтом та сервером під час встановлення з'єднання. Клієнт передає серверу список підтримуваних криптографічних наборів, а сервер обирає один із них для захисту інформації.

Сервери не повинні застосовувати криптографічні набори, які не використовують шифрування або коли для шифрування використовується алгоритм RC4 (у ролі EncryptionAlg встановлено NULL або RC4).

Для шифрування інформації повинні використовуватися симетричні криптографічні алгоритми з довжиною ключа не менш як 128 біт.

Не рекомендується застосовувати криптографічні набори, які для обміну ключами застосовують статичний RSA. Довжина відкритого ключа RSA повинна бути не меншою ніж 2048 біт. Заборонено застосовувати криптографічні набори, які використовують попередньо узгоджений загальний секретний ключ (PSK).

Для узгодження сеансових ключів використовуються протоколи DHE та ECDHE. Довжина відкритого ключа для протоколу DH повинна бути не меншою ніж 2048 біт. Довжина відкритого ключа для протоколу ECDHE повинна бути не меншою ніж 256 біт.

Рекомендується використовувати такі криптографічні набори:

TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256;

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256;

TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384;

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384.

Абоненти-надавачі послуг, абоненти-ідентифікатори, центральний вузол Системи BankID НБУ використовують сертифікати відкритих ключів розширеної перевірки (Extended Validation Certificates, далі – EV SSL сертифікат) у форматі X.509 версії 3.

Рекомендується використовувати браузері провідних розробників (таких як Apple, Google Inc., Microsoft Corporation, Mozilla Foundation, Opera Software ASA) та отримувати EV SSL сертифікати від центрів сертифікації ключів (certificate authority/CA), довірених для відповідних браузерів.

EV SSL сертифікат не повинен мати тип Wildcard. У розширенні “Додаткові дані підписувача” (“subjectAlternativeName”) EV SSL сертифіката не допускається використання URL, який відрізняється від URL, зазначеного в “реквізиті підписувача” (“commonName”) поля “Підписувач” (“subject”).

### **3.3. Вимоги до забезпечення конфіденційності та контролю цілісності електронної анкети**

Абонент-ідентифікатор (банк) перед передаванням електронного підтвердження ідентифікації з інформацією про користувача через Систему BankID НБУ послідовно виконує такі операції:

накладає на електронне підтвердження ідентифікації кваліфіковану електронну печатку;

шифрує підписане електронне підтвердження ідентифікації з використанням кваліфікованого сертифіката шифрування того абонента-надавача послуг, якому передає електронну анкету.

Абонент ідентифікатор має право замість кваліфікованої електронної печатки накладати на електронне підтвердження ідентифікації кваліфікований електронний підпис уповноваженої особи абонента-ідентифікатора (кваліфікований сертифікат у такому випадку повинен бути виданий фізичній особі-представнику абонента-ідентифікатора із внесенням відповідних даних у поля сертифіката, зокрема, кода ЄДРПОУ установи).

Шифрування/розшифрування електронного підтвердження ідентифікації відбувається згідно з алгоритмами та правилами, визначеними Вимогами до форматів криптографічних повідомлень, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 (<http://zakon3.rada.gov.ua/laws/show/z0108-13>). Узгодження ключів шифрування за замовчуванням здійснюється з використанням статичного механізму. Якщо параметри криптографічного алгоритму статичної ключової пари відправника не еквівалентні параметрам криптографічного алгоритму статичної ключової пари одержувача, має здійснюватися перехід до застосування динамічного механізму узгодження ключів.

Абонент-ідентифікатор накладає на електронне підтвердження ідентифікації свою кваліфіковану електронну печатку із використанням формату CAdES-X Long відповідно до ДСТУ ETSI TS 101 733:2017 (ETSI TS 101 733:2013, IDT).