Національний банк України
Рада Системи BankID Національного банку України

ЗАТВЕРДЖЕНО
Рішення Ради Системи BankID
Національного банку України
протокол від 05.11.2021
№ В/57-0007/95807 (зі змінами)
(протокол від 04.02.2022 №В/57-0003/11271, протокол від 22.02.2022 №В/57-0003/16644)

СПЕЦИФІКАЦІЯ ВЗАЄМОДІЇ
абонентського вузла з центральним вузлом Системи BankID Національного банку України

Версія 1.1

Київ 2022

ЗМІСТ

Глосарій

№ з/п	Термін, скорочення	Визначення
1	Абонент Системи BankID НБУ (далі – Абонент)	Абонент-надавач послуг та/або Абонент-ідентифікатор.
2	Абонент-надавач послуг	Юридична особа-резидент приватного або публічного права, яка має укладену з Національним банком України (далі – Національний банк) Публічну пропозицію НБУ на укладення договору приєднання до Системи BankID НБУ, затверджена рішенням Ради Системи BankID НБУ від 26.05.2021 протокол № В/57-0012/41146 (далі – Договір приєднання) та отримує персональні дані користувача Системи BankID НБУ (далі – користувач) засобами Системи BankID НБУ і надає послуги цьому користувачу на території України.
3	Абонент-ідентифікатор	Банк України (далі – Банк), який є Абонентом Системи BankID НБУ та безпосередньо виконує функції ідентифікації, автентифікації та верифікації клієнтів (Банку), які є користувачами.
4	Абонентський вузол Системи BankID НБУ (далі – абонентський вузол)	Комплекс програмно-технічних засобів, установлений в Абонента та призначений для забезпечення обміну інформацією між Абонентами через Систему BankID Національного банку.
5	Авторизація	Процес надання користувачу прав на виконання певних дій або доступу до ресурсів, а також процес перевірки (підтвердження) прав під час спроби виконання цих дій.
6	Автентифікація	Це електронна процедура, що дає змогу підтвердити електронну дистанційну ідентифікацію користувача.
7	Інтернет-банкінг (в т.ч. мобільний банкінг) (далі – ІБ)	Технологія дистанційного банківського обслуговування, яка надає доступ до рахунків та можливості здійснення банківських операцій, доступна користувачу за допомогою браузера (Chrome, Mozilla, Safari, Opera, Edge) та/або мобільного застосунку банку з будь-якого пристрою, який має вихід в Інтернет.
8	Електронна дистанційна ідентифікація – (далі – ідентифікація)	Процес розпізнавання фізичної особи Абонентом-надавачем послуг із підтвердженням успішної автентифікації користувача Системи BankID Національного банку Абонентом-ідентифікатором.

9	Кваліфікований сертифікат шифрування	Сертифікат відкритого ключа, виданий кваліфікованим надавачем довірчих послуг, перелік яких доступний на вебсайті Центрального засвідчуючого органу Міністерства цифрової трансформації України https://www.czo.gov.ua/ca-registry.
10	Кваліфікований електронний підпис (далі - КЕП)	Відповідно до Закону України «Про електронні довірчі послуги» — удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа.
11	Кваліфікована електронна печатка	Відповідно до Закону України «Про електронні довірчі послуги» — удосконалена електронна печатка, яка створюється з використанням засобу кваліфікованої електронної печатки і базується на кваліфікованому сертифікаті електронної печатки.
12	Портал послуг	Вебсайт (вебпортал), мобільний застосунок Абонента-надавача послуг, на якому ініціюється електронний запит на електронну дистанційну ідентифікацію
13	Центральний вузол Системи BankID НБУ (далі – Центральний вузол)	Комплекс програмно-технічних засобів, що забезпечує взаємодію абонентських вузлів Абонентів.
14	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 від Абонента-ідентифікатора до Абонента-надавача послуг, через єдиний вузол, яким виступає Центральний вузол, а також здійснює облік кількості та обсягу наданих Абонентам послуг з електронної дистанційної ідентифікації.
15	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. У Системі BankID НБУ використовується протокол версії 2.0.

1. Загальна частина

1.1. Призначення документа

Опис функціональних вимог та процесу взаємодії абонентських вузлів, а саме Абонента-надавача послуг та Абонента-ідентифікатора із Центральним вузлом.

1.2. Цілі створення системи

Для забезпечення надійної та зручної ідентифікації користувачів шляхом обміну електронними запитами на ідентифікацію та даними між абонентськими вузлами з використанням Центрального вузла, який виконує функцію маршрутизатора.

1.3. Концепція функціонування системи

Функціонування Системи BankID НБУ — це взаємодія трьох складових частин:

1. Абонентський вузол Абонента-надавача послуг;
2. Центральний вузол;
3. Абонентський вузол Абонента-ідентифікатора.

1. **Абонентський вузол Абонента-надавача послуг —** це комплекс програмно-технічних засобів, на якому розміщені програмні процедури електронного запиту/передачі даних до Центрального вузла на базі протоколу OAuth2.0.

Електронний запит на електронну дистанційну ідентифікацію ініціюється на порталі послуг Абонента-надавача послуг, на якому розміщенні форми надання послуг у електронному вигляді. Під час авторизації або замовлення послуги на порталі послуг Абонента-надавача послуг користувачу доступна можливість авторизації або ідентифікації з використанням Системи BankID НБУ у вигляді кнопки на якій зображено логотип Системи BankID НБУ (https://bank.gov.ua/admin_uploads/article/Logo_BankID.zip) та яка може мати підпис “Ідентифікація/Верифікація з використанням Системи BankID НБУ”.

Приклад:

“Ідентифікація/Верифікація з використанням Системи BankID НБУ”

Після натискання кнопки з логотипом Системи BankID НБУ користувач із абонентського вузла Абонента-надавача послуг буде переадресований на абонентський вузол Абонента-ідентифікатора одним із способів:

- через вебсторінку Центрального вузла (https://id.bank.gov.ua/?sidBi), на якій користувач повинен обрати Банк, клієнтом якого він є;
- через пряме посилання до конкретного Банку, якщо перелік Банків відображається на порталі послуг Абонента-надавача послуг. Таким чином у запиті абонентського вузла Абонента-надавача послуг необхідно передати відповідний параметр з ідентифікатором Банку (приклад наведено у п. 2.1.1.).

Абонент-надавач послуг при використанні на своєму порталі послуг способу прямого посилання зобов'язаний відобразити перелік Банків у тій послідовності, як зазначено у переліку Абонентів-ідентифікаторів за посиланням (https://id.bank.gov.ua/api/banks, ключ "order") та забезпечити можливість користувачу вільного вибору Банку. Логотипи та/або назви всіх Банків на порталі послуг Абонента-надавача послуг повинні бути розміщені в єдиному стилі, а саме з пропорційними розмірами та однаковими шрифтами для забезпечення рівноцінного візуального їх сприйняття користувачем.

На порталі послуг Абонента-надавача послуг користувач повинен бути ознайомлений з повним переліком персональних даних, які будуть запитуватися про нього і надати згоду на обробку персональних даних шляхом проставлення відповідної позначки у явному вигляді. Також, користувач повинен бути ознайомлений з розміром плати за передавання та отримання його ідентифікаційних даних та надати свою згоду, якщо таку плату сплачуватиме користувач.

2. **Центральний вузол —** це комплекс програмно-технічних засобів, на якому розміщена вебсторінка з переліком Банків (Абонентів-ідентифікаторів) для подальшого вибору користувачем та програмні процедури обміну інформацією між абонентськими вузлами Абонентів на базі протоколу OAuth2.0.

Після вибору Банку користувач переадресовується до абонентського вузла Абонента-ідентифікатора, на якому користувач, як клієнт Банку, проходить процедуру багатофакторної автентифікації (наприклад, вводить логін та пароль доступу до ІБ та код підтвердження з SMS-повідомлення, яке йому було направлено Абонентом-ідентифікатором на його фінансовий номер).

Після успішного проходження процедури багатофакторної автентифікації, користувач переадресовується для отримання послуги на портал послуг Абонента-надавача послуг, а між Центральним вузлом, абонентським вузлом Абонента-надавача послуг та абонентським вузлом Абонента-ідентифікатора відбувається автоматична взаємодія шляхом отримання/передачі коду авторизації (**authorization_code**), коду доступу (**access_token**) та персональних даних користувача.

3. **Абонентський вузол Абонента-ідентифікатора** (ІБ або інший сервіс банку) — це комплекс програмно-технічних засобів, на стороні якого повинна бути реалізована форма багатофакторної автентифікації користувача,

програмні процедури обміну інформацією на базі протоколу OAuth2.0, автоматичного формування коду авторизації (**authorization_code**), коду доступу (**access_token**), перевірки сертифіката Абонента-надавача послуг, формування електронної анкети (п. 2.3.1.), накладення на неї кваліфікованої електронної печатки Банку, шифрування електронної анкети та переспрямування підписаної і зашифрованої анкети до Абонента-надавача послуг.

Користувач, перейшовши на абонентський вузол Абонента-ідентифікатора має пройти процедуру багатофакторної автентифікації.

Абонентський вузол Абонента-ідентифікатора, на якому користувач проходить процедуру автентифікації та погоджує процес передачі персональних даних, повинен містити назву Банку (Абонента-ідентифікатора), назву його торговельної марки та контактний телефон гарячої лінії з можливістю здійснення переходу користувача безпосередньо на вебсторінку з контактною інформацією відповідного Банку або формою зворотного зв'язку.

Абонент-ідентифікатор зобов'язаний здійснювати багатофакторну автентифікацію користувача, за кожним електронним запитом на електронну дистанційну ідентифікацію до моменту передачі коду авторизації (**authorization_code**).

У разі успішної багатофакторної автентифікації користувач автоматично переадресовується через Центральний вузол на портал послуг Абонента-надавача послуг для продовження процедури отримання послуги. Абонентський вузол Абонента-ідентифікатора здійснює взаємодію з Центральним вузлом згідно з цією специфікацією.

У разі неуспішної багатофакторної автентифікації Абонент-ідентифікатор зобов'язаний інформувати користувача на власному абонентському вузлі щодо конкретної причини відмови у авторизації/ідентифікації (приклад повідомлення про причини відмови: «Перевищено максимальну кількість спроб введення паролю», тощо), не переспрямовувати неавторизованих клієнтів до Центрального вузла та інформувати клієнта про подальші дії (наприклад: «Не вдалося завершити ідентифікацію. Повторіть спробу або зверніться до Банку»).

2. Технічна архітектура системи

Взаємодія Центрального вузла з абонентськими вузлами Абонентів (Рис. 1) відбувається на базі протоколу OAuth2.0 згідно з відповідною специфікацією (опублікована за посиланням https://datatracker.ietf.org/doc/html/rfc6749). Рекомендовано використовувати готові рішення з вебсайту https://oauth.net/2/ – розділ "*Code and Services"*, варіанти під усі популярні платформи та мови програмування.

Автентифікація користувача відбувається засобами абонентського вузла Абонента-ідентифікатора. На персональні дані користувача, що передаються,

накладається кваліфікована електронна печатка Банку і шифруються відповідно до вимог зазначених у п. 3.3.

Логіка роботи Системи BankID НБУ побудована на організації звернень від абонентського вузла Абонента-надавача послуг до абонентського вузла Абонента-ідентифікатора через єдиний шлюз, яким виступає Центральний вузол. Усі абонентські вузли Абонентів взаємодіють виключно через Центральний вузол.

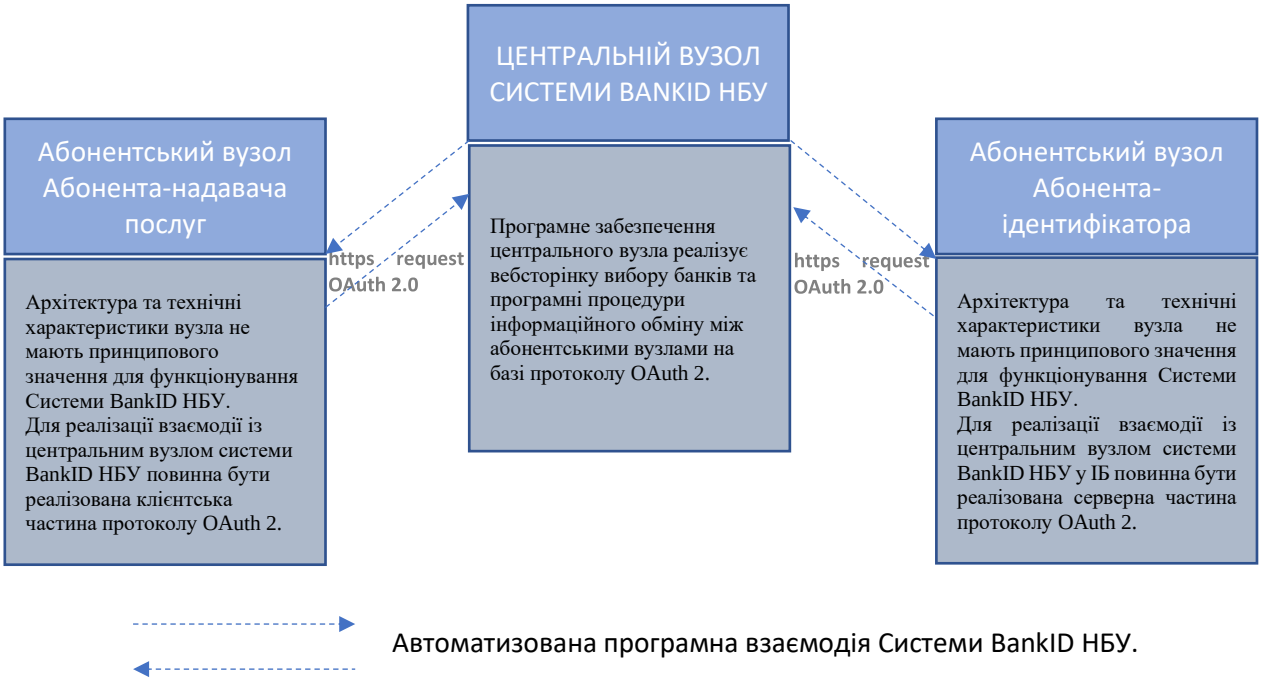

Рис. 1. Технологічна схема функціонування Системи BankID НБУ

Авторизація згідно зі стандартом OAuth 2.0 виконується у два етапи:
перший етап — отримання коду авторизації (**authorization_code)**;
другий етап — отримання коду доступу (**access_token**) на підставі коду авторизації (**authorization_code)**.

2.1. Взаємодія абонентського вузла Абонента-надавача послуг з Центральним вузлом

При підключенні до Системи BankID НБУ Абонент-надавач послуг надає параметр **callback_url** — адреса, на яку будуть виконуватися запити з кодом авторизації (у даному запиті відбувається переадресація користувача). У відповідь адміністратор Системи BankID НБУ надає **client_id** та **client_secret**.

Параметр	Опис
client_id, client_secret	Унікальні ідентифікатори абонентського вузла.
callback_url	Адреса абонентського вузла Абонента-надавача послуг, на яку буде виконано запит з кодом авторизації (**authorization_code**) від Центрального вузла і яка повинна містити домен порталу послуг цього Абонента-надавача послуг, який зазначений у рішенні Ради Системи BankID НБУ (якщо інше не вказане в рішенні Ради Системи BankID НБУ).

2.1.1. Запит до Центрального вузла методом GET на отримання коду авторизації (перший етап)

Запит формується під час переадресації користувача після натискання кнопки на якій зображено логотип Системи BankID НБУ та яка може мати підпис “Ідентифікація/Верифікація з використанням Системи BankID НБУ” на порталі послуг Абонента-надавача послуг.

Приклад структури запиту від абонентського вузла Абонента-надавача послуг до Центрального вузла з параметром банку:

```
curl -X GET "https://id.bank.gov.ua/v1/bank/oauth2/authorize?
   response_type=code&
   client_id=client_id&
   state=state&
   bank_id=id"
```

Приклад структури запиту, який застосовується виключно для абонентського вузла Інтегрованої системи електронної ідентифікації ДП “ДІЯ” до Центрального вузла з параметром банку:

```
curl -X GET "https://id.bank.gov.ua/v1/bank/oauth2/authorize?
   response_type=code&
   client_id=client_id&
   state=state&
   bank_id=id&
   originator_id=edrpou_code&
   originator_url=url"
```

Відповідь Центрального вузла у випадку якщо запит виконано з параметром банку (**bank_id**), що підключений до Системи BankID НБУ:

```
HTTP/1.1 200 OK
Запит від абонентського вузла Абонента-надавача послуг проходить через Центральний вузол і направляється на абонентський вузол обраного Банку для проходження подальшої автентифікації користувача в системі Банку.
```

Приклад структури запиту від абонентського вузла Абонента-надавача послуг до Центрального вузла без параметра Банку:

```
curl -X GET "https://id.bank.gov.ua/v1/bank/oauth2/authorize?
   response_type=code&
   client_id=client_id&
   state=state"
```

Відповідь Центрального вузла у випадку якщо запит виконано без параметра банку:

```
HTTP/1.1 200 OK
Перехід на вебсторінку Центрального вузла, на якій доступний перелік Банків (абонентських вузлів Абонентів-ідентифікаторів), що підключені до Системи BankID НБУ.
```

Параметр	Опис
response_type	Значення повинно бути **“code”**.
client_id	Ідентифікатор абонентського вузла отриманий при підключенні (п. 2.1.).
state	Унікальний ідентифікатор сесії. Довільне значення параметра, генерується з боку абонентського вузла Абонента-надавача послуг і буде повернуто в запиті з кодом авторизації. Не більше 50 знаків.
bank_id	Ідентифікатор абонентського вузла Абонента-ідентифікатора. Параметр необов’язковий, використовується у випадку якщо Абонент-ідентифікатор обирається безпосередньо на порталі послуг Абонента-надавача послуг. Значення має бути обрано із ключа «**id**» (детальний опис у п. 2.4.).

originator_id	Унікальний ідентифікаційний номер юридичної особи в Єдиному державному реєстрі підприємств та організацій України (код ЄДРПОУ), яка ініціює запит на інформацію. Не більше 8 цифр. Використовується виключно для “Інтегрована система електронної ідентифікації **ID.GOV.UA**”.
originator_url	Адреса порталу послуг юридичної особи від якого ініціюється запит на інформацію (наприклад, https://mvs.gov.ua). Використовується виключно для “Інтегрована система електронної ідентифікації **ID.GOV.UA**”.

У разі успішної багатофакторної автентифікації користувача на стороні Абонента-ідентифікатора Центральний вузол виконує запит до абонентського вузла Абонента-надавача послуг із кодом авторизації **authorization_code** на зареєстрований параметр **callback_url**.

Приклад структури запиту з кодом авторизації від Центрального вузла до абонентського вузла Абонента-надавача послуг:

```
curl -X GET "https://portal.example.com.ua/v1/bank/oauth2/callback/code?
   code=authorization_code&
   state=state"
```

Параметр	Опис
code	Код авторизації (**authorization_code**) — унікальний ідентифікатор, який формується на стороні Центрального вузла. Час дії коду 90 секунд.
state	Значення параметра, яке передав абонентський вузол Абонента-надавача послуг у першому GET запиті до Центрального вузла.

Можливі помилки

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

- абонентський вузол Абонента-надавача послуг не вдалося ідентифікувати, зокрема, абонентський вузол не зареєстрований на стороні Центрального вузла, або не співпадає значення певного параметра в запиті, або взаємодію з цим абонентським вузлом призупинено. У такому випадку опис помилки буде відображено на вебсторінці Центрального вузла;
- користувача не вдалося автентифікувати на стороні Абонента-ідентифікатора. В такому випадку причина помилки має відображатися користувачу на стороні Абонента-ідентифікатора.

2.1.2. Запит до Центрального вузла на отримання коду доступу (access_token) методом POST (другий етап)

Після отримання коду авторизації (**authorization_code**) абонентський вузол Абонента-надавача послуг повинен виконати запит на отримання коду доступу (**access_token**).

Приклад структури запиту від абонентського вузла Абонента-надавача послуг до Центрального вузла на код доступу:

```
curl -X POST "https://id.bank.gov.ua/v1/bank/oauth2/token"
     -H "Content-Type: application/x-www-form-urlencoded"
     -d "grant_type=authorization_code&
         client_id=client_id&
         client_secret=client_secret&
         code=authorization_code"
```

Параметр	Опис
grant_type	Значення повинно бути **“authorization_code”**.
client_id, client_secret	Ідентифікатори абонентського вузла Абонента-надавача послуг, які були отримані при підключенні (п. 2.1.).
code	Значення коду авторизації (**authorization code**), отриманого від Центрального вузла на попередньому кроці (п. 2.1.1.).

У відповідь Центральний вузол надає код доступу в тілі (*body*) запиту у Json-форматі. Структура відповіді Центрального вузла:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
   "token_type": "bearer",
   "access_token": "access_token",
   "expires_in": 180
}
```

Параметр	Опис
token_type	Значення повинно бути **“bearer”**.
access_token	Значення коду доступу.
expires_in	Термін дії коду доступу (значення в секундах), матиме значення 180.

Можливі помилки

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

Приклад тіла (*body*) відповіді з помилкою:

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

Параметр	Опис
error	Один із визначених кодів помилки згідно специфікації OAuth2.0 (https://tools.ietf.org/html/rfc6749#section-5.2). Зокрема: **invalid_client** – у запиті некоректно вказані ідентифікатори абонентського вузла Абонента-надавача послуг (client_id/client_secret); **invalid_request** – у запиті немає обов'язкових значень одного або декількох параметрів; **invalid_grant** – некоректний код авторизації (authorization_code) або термін дії коду авторизації завершився.
error_description	Текстовий опис помилки, деталізація для розробників.
code	Значення коду авторизації (**authorization_code**) при якому виникла помилка.

2.2. Взаємодія абонентського вузла Абонента-ідентифікатора з Центральним вузлом

При підключенні до Системи BankID НБУ Абонент-ідентифікатор надає вебадреси **login_url, token_api_url** та **data_api_url**. У відповідь адміністратор Системи BankID НБУ надає **client_id** та **client_secret**.

Параметр	Опис
client_id, client_secret	Унікальні ідентифікатори абонентського вузла.

login_url	Вебадреса абонентського вузла, на яку буде переадресовано користувача для подальшого проходження користувачем автентифікації в системі Абонента-ідентифікатора. Адміністраторами Системи BankID НБУ вебадреса буде доповнена параметрами та значеннями згідно наданого у п. 2.2.1. прикладу структури запиту від Центрального вузла до абонентського вузла Абонента-ідентифікатора.
token_api_url	Вебадреса абонентського вузла, на яку здійснюватиметься запит для отримання коду доступу (**access_token**).
data_api_url	Вебадреса абонентського вузла, на яку здійснюватиметься запит для отримання персональних даних користувача.

2.2.1. Запит до абонентського вузла Абонента-ідентифікатора методом GET і отримання коду авторизації (перший етап)

Запит формується під час переадресації користувача від Центрального вузла до абонентського вузла Абонента-ідентифікатора.

Приклад структури запиту від Центрального вузла до абонентського вузла Абонента-ідентифікатора:

```
curl -X GET "https://bank.example.com.ua/v1/bank/oauth2/authorize?
    response_type=code&
    client_id=client_id&
    state=state"
```

Параметр	Опис
response_type	Значення повинно бути **“code”**.
client_id	Ідентифікатор абонентського вузла отриманий при підключенні (п. 2.2.).
state	Унікальний ідентифікатор сесії. Генерується з боку Центрального вузла і має бути повернутий абонентським вузлом у запиті з кодом авторизації.

Відповідь Абонента-ідентифікатора:

```
HTTP/1.1 200 OK
Перехід на вебсторінку абонентського вузла Абонента-ідентифікатора для подальшої автентифікації користувача в ІБ Банку.
```

У разі успішної автентифікації користувача Абонентом-ідентифікатором абонентський вузол Абонента-ідентифікатора здійснює запит до Центрального вузла із кодом авторизації (**authorization_code)** на вебадресу **callback_url**. Із даним запитом відбувається переадресація користувача на Центральний вузол.

Приклад структури запиту з кодом авторизації від абонентського вузла Абонента-ідентифікатора до Центрального вузла:

```
curl -X GET "https://id.bank.gov.ua/v1/bank/oauth2/callback/code?
   code=authorization_code&
   state=state"
```

Параметр	Опис
callback_url	Вебадреса Центрального вузла (https://id.bank.gov.ua/v1/bank/oauth2/callback/code), на яку абонентський вузол Абонента-ідентифікатора здійснить запит із кодом авторизації (**authorization_code**) та переадресацію користувача.
code	Код авторизації (**authorization_code**) — унікальний ідентифікатор, який формується на стороні Абонента-ідентифікатора. Час дії коду 90 секунд.
state	Буде вказано значення параметру, яке передав Центральний вузол у першому GET запиті.

Можливі помилки

Якщо на даному етапі користувача не вдалося автентифікувати на стороні Абонента–-ідентифікатора або сталася якась інша помилка, то причина помилки має відображатися користувачу на стороні Абонента-ідентифікатора і у такому разі переадресовувати користувача до Центрального вузла не потрібно.

2.2.2. Запит до абонентського вузла Абонента-ідентифікатора на отримання коду доступу (access_token) методом POST (другий етап)

Після отримання коду авторизації (**authorization_code**) Центральний вузол виконує запит на отримання коду доступу (**access_token**).

Приклад структури запиту від Центрального вузла до абонентського вузла Абонента-ідентифікатора:

```
curl -X POST "https://bank.example.com.ua/v1/bank/oauth2/token"
     -H "Content-Type: application/x-www-form-urlencoded"
```

```
-d "grant_type=authorization_code&
    client_id=client_id&
    client_secret=client_secret&
    code=authorization_code"
```

Параметр	Опис
grant_type	Значення повинно бути **“authorization_code”**.
client_id, client_secret	Ідентифікатори абонентського вузла отримані при підключенні (п. 2.2.).
code	Значення коду авторизації (**authorization code**), отриманого від Абонента-ідентифікатора на попередньому кроці (п. 2.2.1.).

У відповідь абонентський вузол Абонента-ідентифікатора надає код доступу в тілі (*body*) запиту у Json-форматі.

Приклад структури відповіді абонентського вузла Абонента-ідентифікатора на запит коду доступу від Центрального вузла:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
   "token_type": "bearer",
   "access_token": "access_token",
   "expires_in": 180
}
```

Параметр	Опис
token_type	Значення повинно бути **“bearer”**.
access_token	Значення коду доступу.
expires_in	Термін дії коду доступу (значення в секундах). Повинен мати значення 180.

Можливі помилки

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

Приклад тіла (*body*) відповіді з помилкою:

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

Параметр	Опис
error	Один із визначених кодів помилки згідно специфікації OAuth2.0 (https://tools.ietf.org/html/rfc6749#section-5.2). Зокрема: **invalid_client** – у запиті некоректно вказані ідентифікатори абонентського вузла (client_id/client_secret); **invalid_request** – у запиті немає обов'язкових одного або декількох параметрів; **invalid_grant** – некоректний код авторизації (authorization_code) або термін дії коду авторизації завершився; **server_error** – інша помилка при обробці запиту на код доступу.
error_description	Текстовий опис помилки, деталізація для розробників.
code	Значення коду авторизації (**authorization_code**), при якому виникла помилка.

2.3. Процедура отримання даних користувача

Надання даних користувача відбувається на підставі коду доступу (**access_token**). Код доступу передається абонентським вузлом Абонента-надавача послуг у заголовку (**headers**) запиту на дані у вигляді:

```
Authorization: "Bearer access_token"
```

Також, Абонент-надавач послуг у запиті на дані до Центрального вузла, повинен вказати, який саме перелік необхідних даних стосовно користувача потрібно отримати та надати свій кваліфікований сертифікат шифрування. Отриманий запит Центральний вузол переспрямовує до абонентського вузла Абонента-ідентифікатора, на якому користувач проходить автентифікацію.

Кваліфікований сертифікат шифрування передається у значенні ключа "**cert**" у форматі DER закодований у BASE64.

Перелік необхідних даних зазначається згідно з допустимими ключами (п. 2.3.1.) у вигляді Json-об’єкту в тілі (*body*) запиту.

Приклад Json-об’єкта тіла (*body*) запиту на дані:

```
{"type": "physical",
 "cert": "Encode to base64 format",
 "memberId": "1111111101",
 "sidBi": "2baeadd0-c7e6-4ad9-9181-1fd9bbebfaac",
 "fields": [
    "firstName", "middleName", "lastName", "phone", "inn", "birthDay", "sex"
 ],
 "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", "issueCountryIso2"
  ]},
  {"type": "zpassport", "fields":[
   "series", "number", "issue", "dateIssue", "dateExpiration", "issueCountryIso2"
  ]}
 ]
}
```

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

2.3.1. Електронна анкета (з переліком та описом допустимих ключів)

Ключ			Значення ** (формат та вимоги)	Опис
1	2	3	4	5
cert*			Формат сертифікату DER, закодовано за стандартом BASE64.	Кваліфікований сертифікат шифрування
memberId			XXXXXXXXNN – де: XXXXXXXX – ідентифікатор абонента (код ЄДРПОУ); NN – порядковий номер	Унікальний ідентифікатор абонентського вузла Абонента в Системі BankID НБУ

Ключ			Значення ** (формат та вимоги)	Опис
1	2	3	4	5
			абонентського вузла. Ключ та значення додаються Центральним вузлом.	
sidBi			Ключ та значення додаються Центральним вузлом.	Ідентифікатор сесії.
type			**physical**	Значення ідентифікації особи. На даний час приймає тільки одне значення – physical
	fields	**Масив з даними по особі**		
		lastName*****		Прізвище
		firstName*****		Ім’я
		middleName*	У разі відсутності по батькові у документах користувача, необхідно передавати значення «**n/a**»*******. Можливі значення: 'по батькові' або 'n/a'.	По батькові
		phone	380XXXXXXXXX – де X може приймати тільки цифрове значення.	Номер телефону
		inn*****	Заповнюється відповідно до вимог законодавства України. Якщо у користувача нерезидента/резидента України відсутній реєстраційний номер облікової картки платника податків, необхідно передавати значення 'n/a'. Можливі значення: 'XXXXXXXXXX' – код, де X може приймати лише цифрове значення; 'NNXXXXXX' - паспорт, де NN – серія, XXXXXX – цифрове значення номеру паспорта; 'XXXXXXXXX' – номер id картки, де X може приймати лише цифрове значення; або 'n/a'.	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 (для нерезидентів та резидентів України заповнюється за наявності у них реєстраційного номеру облікової картки платника податків).
		clId		Унікальний ідентифікатор особи (клієнта) в банку. У випадку якщо банк не має такого ідентифікатора, можливо вказати значення ключа inn або серію і номер паспорта.
		clIdText	“Інформація надана з використанням Системи BankID НБУ dd.mm.yyyy hh.mm”	Статичний текст з інформацією про надані дані Абонентом-ідентифікатором щодо особи, дата і час надання
		birthDay*****	dd.mm.yyyy	Дата народження
		birthPlace	Можливі значення: 'UA'/	Країна народження

Ключ			Значення ** (формат та вимоги)	Опис
1	2	3	4	5
			'UKR' (літерний код країни за стандартом ISO_3166-1 (alfa-2/alfa-3) або 'Україна'/'Ukraine'.	
		nationality	Можливі значення: 'UA'/ 'UKR' (літерний код країни за стандартом ISO_3166-1 (alfa-2/alfa-3) або 'Україна'/'Ukraine'.	Громадянство
		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
		workPlace		Місце роботи. (заповнюється для соціального статусу **«працюючий»** або **«нерегулярна зайнятість»**)
		position		Посада (заповнюється для соціального статусу **«працюючий»** або **«нерегулярна зайнятість»**)
		flagPEPs	Можливі значення: 1 – так, 0 – ні.	Ознака, чи визначена особа повіреною Абонентом-ідентифікатором такою, що належить до категорії PEPs (публічні особи, близькі, пов’язані)
		flagPersonTerror	Можливі значення: 1 – так, 0 – ні.	Ознака, чи визначена особа повіреною Абонентом-ідентифікатором 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 особа повіреною Абонентом-ідентифікатором 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 присвоєно особі повіреною Абонентом-ідентифікатором (неприйнятно) високий рівень ризику ПВК/ФТ
		uaResident	Можливі значення: 1 – так, 0 – ні.	Ознака, чи визначена особа повіреною Абонентом-ідентифікатором такою, що є резидентом України

Ключ			Значення ** (формат та вимоги)	Опис
1	2	3	4	5
		phoneNumberChange	dd.mm.yyyy	Дата встановлення або дата зміни фінансового номеру телефону в системах Абонента-ідентифікатора
		identificationDate	dd.mm.yyyy	Дата проходження ідентифікації особою
addresses	**Масив типів адрес та адресних даних особи**			
	type*		Можливі значення: **factual,** **juridical.**	Тип адреси проживання: **factual** – фактична адреса проживання; **juridical –** адреса реєстрації.
	fields	**Масив адресних даних особи**		
		country*	Можливі значення: 'UA'/ 'UKR' (літерний код країни за стандартом ISO_3166-1 (alfa-2/alfa-3) або 'Україна'/'Ukraine'.	Країна проживання/реєстрації
		index	'XXXXX' – де X може приймати тільки цифрове значення	Поштовий індекс
		state*	Якщо адреса користувача не передбачає наявності області, необхідно передавати значення 'n/a'. Можливі значення: 'назва області' або 'n/a'.	Область
		area*	Якщо адреса користувача не передбачає наявності району, необхідно передавати значення 'n/a'. Можливі значення: 'назва району' або 'n/a'.	Район
		city*		Назва населеного пункту
		street*	Якщо адреса користувача не передбачає наявності типу вулиці (наприклад: вулиця, узвіз, проспект і тд) та її назви, необхідно передавати значення 'n/a'. Можливі значення: 'тип вулиці та її назва' або 'n/a'.	Тип вулиці (наприклад: вулиця, узвіз, проспект і тд) та її назва
		houseNo*	Якщо адреса користувача не передбачає наявності номеру будинку, необхідно передавати значення 'n/a'. Можливі значення: 'номер будинку' або 'n/a'.	Номер будинку (і за наявності літера будинку та/або номер корпусу/блоку/секції)
		flatNo*	Якщо адреса користувача не передбачає наявності номеру квартири, необхідно передавати значення 'n/a'. Можливі значення: 'номер квартири' або 'n/a'.	Номер квартири (і за наявності літера квартири)
documents	**Масив типів документів та реквізити документів, що посвідчують особу**			
	type*		Можливі значення: **passport,**	Тип документу: **passport** – паспорт

Ключ			Значення ** (формат та вимоги)	Опис
1	2	3	4	5
			idpassport, **zpassport,** **ident.**	громадянина України; **idpassport** – id-картка; **zpassport** – паспорт для виїзду за кордон; **ident** – інший документ, що посвідчує особу та відповідно до законодавства України може бути використаний на території України для укладення правочинів Свідоцтво про народження не є документом типу ident.
	fields	**Масив реквізитів документів, що посвідчують особу**		
		typeName		Назва документу
		series*	Якщо документ особи не передбачає наявності серії документу, необхідно передавати значення 'n/a'. Можливі значення: 'серія' або 'n/a'.	Серія документа
		number*		Номер документа
		issue*		Яким органом видано документ
		dateIssue*	dd.mm.yyyy	Дата видачі документу
		dateExpiration*	Якщо документ особи не передбачає наявності терміну дії, необхідно передавати значення 'n/a'. Можливі значення: 'dd.mm.yyyy' або 'n/a'	Термін дії
		recordEDDR	Заповнюється відповідно до вимог законодавства України: 'XXXXXXXX-XXXXX' – код, де X може приймати лише цифрове значення.	Унікальний номер запису в Єдиному державному демографічному реєстрі (для типу **passport** не заповнюється, для типів **zpassport** та **ident** - заповнюється за наявності інформації у документах особи)
		issueCountryIso2	Можливі значення: 'UA'/ 'UKR' (літерний код країни за стандартом ISO_3166-1 (alfa-2/alfa-3) або 'Україна'/'Ukraine'.	Країна видачі документа

* — обов’язкові ключі для заповнення Абонентом-ідентифікатором.
** — всі значення ключів мають символьний тип.
*** — у Системі BankID НБУ скорочення 'n/a' використовується у значенні не застосовується (англ. not applicable).

2.3.2. Вимоги щодо передачі Абонентом-ідентифікатором персональних даних користувача, як клієнта Банку

Дані клієнта, передані через Центральний вузол у відповіді від Абонента-ідентифікатора вважаються такими, що відповідають вимогам цієї специфікації у випадку виконання наступних вимог.

Абонент-ідентифікатор зобов'язаний передати дані клієнта за ключами, що позначені в Електронній анкеті (п. 2.3.1), як обов'язкові до заповнення та містяться у електронному запиті на ідентифікацію Абонента-надавача послуг.

Якщо дані клієнта за обов'язковими ключам відсутні у його документах, то Абонент-ідентифікатор зобов'язаний передати значення «n/a» у своїй відповіді (застосовується до ключів в значеннях яких дозволено передавати «n/a»). У разі невиконання цих умов Абонентом-ідентифікатором, електронне підтвердження електронної дистанційної ідентифікації вважається таким, що не відповідає вимогам цієї специфікації і може бути оскаржене Абонентом-надавачем послуг та визнане таким, що не підлягає тарифікації за міжабонентськими тарифами.

Абоненту-ідентифікатору забороняється передавати дані тих клієнтів, щодо яких у Абонента-ідентифікатора є підстави для здійснення заходів щодо актуалізації їх даних. Абоненту-ідентифікатору необхідно здійснити процедуру актуалізації даних про таких клієнтів у строки, які встановлені законодавством з питань фінансового моніторингу. В такому випадку Абонент-ідентифікатор має проінформувати користувача щодо такої необхідності відповідним повідомленням під час здійснення процедури багатофакторної автентифікації. У разі невиконання цієї умови Абонентом-ідентифікатором, електронне підтвердження електронної дистанційної ідентифікації вважається таким, що не відповідає вимогам цієї специфікації і може бути оскаржене Абонентом-надавачем послуг та визнане таким, що 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 Абонентом-ідентифікатором та не є предметом оскарження.

За запитом Абонента-надавача послуг на отримання даних клієнта за усіма документами (ключ "documents"), Абонент-ідентифікатор зобов'язаний передати дані по клієнту лише за актуальним(и) документом(ами) та не менше ніж за одним із документів: паспорт громадянина України ("passport"), id-картка ("idpassport"), паспорт для виїзду за кордон ("zpassport"), інший документ, що посвідчує особу та відповідно до законодавства України може бути використаний на території України для укладення правочинів ("ident"). За запитом абонента-надавача послуг на отримання даних клієнта за окремим(и) документом(ами), тобто не за усіма документами (ключ "documents"), Абонент-ідентифікатор зобов'язаний передати дані по клієнту лише за актуальним(и) документом(ами) та не менше ніж за одним із запитуваних документів у разі наявності такого(их) документу(ів) у Абонента-ідентифікатора. Якщо клієнта

ідентифіковано та верифіковано на підставі іншого документу, який Абонент-надавач послуг не зазначив у запиті, Абонент-ідентифікатор у такому випадку нічого не передає у значенні ключа "documents". Інформація надана Абонентом-ідентифікатором у відповідності до цих вимог, вважається такою що надана у повному обсязі відповідно до вимог цієї специфікації. Абоненту-ідентифікатору забороняється передавати дані тих клієнтів, які були ним ідентифіковані та верифіковані на підставі лише свідоцтва про народження. Якщо відповідь абонента-ідентифікатора за ключем "documents" містить одночасно дані за актуальним документом та неактуальним документом, або містить лише дані свідоцтва про народження, то таке електронне підтвердження електронної дистанційної ідентифікації вважається таким, що не відповідає вимогам цієї специфікації і може бути оскаржене Абонентом-надавачем послуг та визнане таким, що не підлягає тарифікації за міжабонентськими тарифами.

Абоненту-ідентифікатору забороняється передавати дані за запитом Абонента-надавача послуг на отримання даних клієнта за документом з масиву типів документів та реквізитів, що посвідчують особу (ключ "documents") якщо на день надходження такого запиту у цього документа закінчився термін дії, тобто дата (термін дії), яка буде зазначена Абонентом-ідентифікатором у значенні ключа "dateExpiration" не може бути меншою (більш ранньою), ніж та, в яку надійшов електронний запит від Абонента-надавача послуг (не застосовується до типу документа "passport"). Невиконання цієї умови Абонентом-ідентифікатором є порушенням вимог цієї специфікації.

Абоненту-ідентифікатору забороняється передавати дані за запитом Абонента-надавача послуг на отримання даних клієнта-малолітньої особи (діти, які не досягли 14 років).

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

за документом паспорт громадянина України ("passport") ключ "dateExpiration" заповнюється значенням «n/a»;

у випадку коли у документах клієнта відсутня серія документа, то значення ключа "series" заповнюється «n/a».

За запитом Абонента-надавача послуг на отримання даних клієнта за двома типами адрес (фактична адреса та адреса реєстрації) ключа "addresses", обов’язковим до передачі є два типи адрес. Якщо у відповіді Абонента-ідентифікатора надано інформацію лише за одним типом адреси, то така інформація є наданою не у повному обсязі та може бути оскаржена Абонентом-надавачем послуг та визнана такою, що не підлягає тарифікації за міжабонентськими тарифами.

Значення ключів “workPlace” та “position” заповнюються абонентом-ідентифікатором виключно на запит банків, зареєстрованих у Системі BankID НБУ у статусі Абонентів-надавачів послуг та можуть бути використані такими Абонентами-надавачами послуг виключно для надання фінансових послуг без права передавання їх третім особам.

Абонент зобов'язаний зберігати електронні запити на електронну дистанційну ідентифікацію користувача та електронні підтвердження електронної дистанційної ідентифікації користувача (значення всіх ключів Електронної анкети (п. 2.3.1.)) в електронному вигляді не менше 5 (п’яти) років після припинення ділових відносин з клієнтом або завершення разової фінансової операції без встановлення ділових відносин з клієнтом, щодо якого Абонентом було надіслано/отримано електронний запит на електронну дистанційну ідентифікацію або надане/отримане електронне підтвердження електронної дистанційної ідентифікації, для можливості вирішення спорів між Абонентами з питань невідповідності успішних електронних підтверджень електронної дистанційної ідентифікації вимогам цієї специфікації.

2.3.3. Запит даних користувача

Для отримання даних щодо користувача, абонентський вузол Абонента-надавача послуг здійснює запит до Центрального вузла. Центральний вузол здійснює перенаправлення запиту до абонентського вузла Абонента-ідентифікатора за вебадресою, наданою Абонентом-ідентифікатором під час реєстрації (**data_api_url** п. 2.2.).

Приклад запиту на дані від Абонента-надавача послуг до Центрального вузла:

```
curl -X POST https://id.bank.gov.ua/v1/bank/resource/client
  -H "Content-Type: application/json" -H "Authorization: Bearer access_token"
  -d '{"type": "physical",
        "cert": "Encode to base64 format",
        "fields":[
           "firstName", "middleName", "lastName",
           "phone", "inn", "clId", "clIdText", "birthDay", "sex"
        ],
        "addresses":[
           {"type": "factual", "fields":[
              "country", "state", "area", "city", "street", "houseNo", "flatNo"
           ]}
        ],
        "documents":[
           {"type": "passport", "fields":[
              "typeName", "series", "number",
              "issue", "dateIssue", "issueCountryIso2"
           ]}
        ]
}'
```

Параметр	Опис
access_token	Код доступу, що отриманий у відповіді на запит (п. 2.2.2.).

Отриманий запит на дані від абонентського вузла Абонента-надавача послуг доповнюється Центральним вузлом ключами/значеннями **memberId**, **sidBi** і перенаправляється до абонентського вузла Абонента-ідентифікатора.

Абонент-ідентифікатор зобов'язаний перевірити чи відповідає код ЄДРПОУ, наданий у сертифікаті запитувача тому, що зазначений у ключі **memberId** (перші 8-цифр). У випадку невідповідності віддавати помилку на запит з описом причини.

Відповідь з даними Абонента-ідентифікатора надається у вигляді Json-об'єкта, в якому Абонент-ідентифікатор надає свій кваліфікований сертифікат шифрування в значенні ключа "**cert**" у форматі DER закодованого BASE64 та цифровий конверт, що містить зашифровані персональні дані користувача, на які накладено кваліфіковану електронну печатку Банку у значенні ключа "**customerCrypto**" у форматі DER закодованого BASE64.

Приклад відповіді:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
  "state": "ok",
  "cert":
"MIIGUDCCBfigAwIBAgIUW2PYg3XZIBgEAAAALj0AALKVAAAwDQYL
KoYkAgEBAQEDAQEwgcMxFjAUBgNVBAoM (part of the base64 example)",
  "customerCrypto":
"MIIdhwYJKoZIhvcNAQcDoIIdeDCCHXQCAQIxggHtoYIB6QIBA6BOoUww
DwYLKoYkAgEBAQEDAQEFAAM5AAQ2rSxwb/DU/xDvLrfRCrT5QwOkUR
/jXRJLPqnVBktn0UTXna4YQRUnv1XT2BRRFY (part of the base64 example)"
}
```

Отримана відповідь від абонентського вузла Абонента-ідентифікатора доповнюється Центральним вузлом ключами/значеннями **memberId**, **sidBi** і перенаправляється абонентському вузлу Абонента-надавача послуг.

Персональні дані Абонент-ідентифікатор формує у стандарті кодування UTF-8 у форматі Json-об'єкту, наприклад:

```
{
   "type": "physical",
   "inn": "112233445566",
```

```
   "sex": "M",
   "email": "geraschenko@gmail.com",
   "birthDay": "20.01.1953",
   "firstName": "ПЕТРО",
   "lastName": "ГЕРАЩЕНКО",
   "middleName": "ІВАНОВИЧ",
   "phone": "380961234511",
   "clId": "6299E05EC5D568733C14CCEF9C975DD3",
   "clIdText": "Інформація надана з використанням 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",
      "typeName": "паспорт",
      "series": "АА",
      "number": "222333",
      "issue": "Ківерцівським РО УМВД",
      "dateIssue": "15.03.1999",
      "dateExpiration": "25.09.2005"
   }]
}
```


Вказаний Json-об’єкт підписується кваліфікованою електронною печаткою Абонента-ідентифікатора і шифрується за алгоритмом визначеним у ДСТУ ГОСТ 28147-2009. Шифрування підписаних персональних даних відбувається згідно з вимогами до форматів криптографічних повідомлень, визначених наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 27.10.2020 № 687 (далі – Вимоги) https://zakon.rada.gov.ua/laws/show/z1272-20#n8. 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 повинні підтримувати криптографічні алгоритми, визначені Вимогами.

Підписаний та зашифрований об’єкт формується у вигляді цифрового конверта згідно з Вимогами і передається у відповіді у значенні ключа "**customerCrypto**" у форматі DER закодованого в BASE64.

Можливі помилки

У разі виникнення помилок оброблення запиту рекомендується 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 (*body*) запиту у Json-форматі.

Приклад помилки:


```
{"error": "invalid_must_key",
 "error_description": "На жаль, у нас немає всіх необхідних даних цього клієнта. Відсутня фактична адреса проживання.",
 "code": "CL003"
}
```


Параметр	Опис
error	Приклади помилок: **invalid_request** – у запиті на отримання персональних даних немає обов’язкових значень одного або декількох параметрів або некоректно зазначені ключі; **invalid_token** – некоректний код доступу (**access_token**) або термін дії коду доступу завершився; **invalid_cert** – проблеми під час оброблення кваліфікованого сертифікату, зокрема некоректний/недійсний сертифікат, що був наданий абонентським вузлом Абонента-надавача послуг; **invalid_must_key** – у Абонента-ідентифікатора відсутня інформація про користувача за обов’язковим(и) ключем (ключами); **invalid_acsk** – виникла помилка при взаємодії Абонента-ідентифікатора з сервером акредитованого центру сертифікації ключів;

	invalid_server – інша помилка на сервері при обробці банком запиту на дані. Приклади помилок, визначених Центральними вузлом: **repeat_request** – вузлом Абонента-надавача послуг здійснено повторний запит на отримання персональних даних; **request_timeout** – термін відповіді Абонента-ідентифікатора на запит даних завершився; **invalid_response** – у відповіді Абонента-ідентифікатора на запит персональних даних немає тіла (body) або тіло відповіді не у Json-форматі.
error_description	Текстовий опис помилки державною мовою. Наприклад: «На жаль, у нас немає всіх необхідних даних цього клієнта: **перелік**»; «Відсутній обов'язковий ключ/ключі: **перелік**»; «Сертифікат недійсний»; «Сертифікат не належить Абоненту»; «Відповідь від OCSP сервера не отримано. **назва центру сертифікації**»; «Виникла помилка при взаємодії банку з OCSP сервером акредитованого центру сертифікації ключів. **назва центру сертифікації**»; «Виникла помилка при взаємодії банку з TSP сервером акредитованого центру сертифікації ключів. **назва центру сертифікації**».
code	Певне значення, яке може допомогти Абоненту-ідентифікатору для аналізу причини помилки.

2.4. Додаткова технічна інформація

У тестовому середовищі Системи BankID НБУ https://testid.bank.gov.ua (на період тестування необхідно використовувати саме це доменне ім'я, в тому числі у запиті з кодом авторизації) взаємодія Центрального вузла із абонентськими вузлами Абонентів здійснюється виключно з використанням унікальних ідентифікаторів, наданих Абоненту адміністратором Системи BankID НБУ для тестування.

У промисловому середовищі Системи BankID НБУ https://id.bank.gov.ua взаємодія Центрального вузла із абонентськими вузлами Абонентів здійснюється виключно з використанням параметрів, які вказані у Договорі

приєднання та унікальних ідентифікаторів, наданих адміністратором Системи BankID НБУ.

Перелік доступних абонентських вузлів Абонентів-ідентифікаторів Системи BankID НБУ у Json-форматі https://id.bank.gov.ua/api/banks

Приклад за одним із Абонентів-ідентифікаторів:


```
{
  "id": "examplebank",
  "name": "Банк",
  "workable": true,
  "memberId": "1234567891",
  "logoUrl": "assets/images/banks/examplebank.png",
  "order": 15
}
```


Ключ	Опис
id	Назва абонентського вузла Абонента-ідентифікатора. Може містити літери латиниці, цифри та дефіс. Значення використовується лише тоді, коли переадресація користувача відбувається через пряме посилання, а не через вебсторінку Центрального вузла.
name	Коротка назва абонентського вузла Абонента-ідентифікатора в Системі BankID НБУ. Назва може містити літери кирилиці, латиниці, цифри та спеціальні знаки.
workable	Ознака роботи абонентського вузла. Значення boolean: true – абонентський вузол працює; false – роботу абонентського вузла призупинено.
memberId	Унікальний ідентифікатор абонентського вузла в Системі BankID НБУ. Складається з цифр: перші 8 – код ЄДРПОУ; останні 2 – порядковий номер абонентського вузла.
logoUrl	Відносне посилання на логотип абонентського вузла Абонента-ідентифікатора розміщеного на вебсторінці Центрального вузла.
order	Порядковий номер абонентського вузла Абонента-ідентифікатора на вебсторінці Центрального вузла.

Перелік Абонентів Системи BankID НБУ у Json-форматі:

- загальний перелік – https://id.bank.gov.ua/v1/api/abonents;

- по значенню ЄДРПОУ Абонента, наприклад, по ЄДРПОУ 37508596 – https://id.bank.gov.ua/v1/api/abonents/?edrpou=37508596;
- по значенню ключа “memberId”, наприклад, “memberId” 3750859601 – https://id.bank.gov.ua/v1/api/abonents/3750859601.

Приклад за одним із Абонентів:


```
{
 "name": "Установа України",
 "edrpou": "12345678",
 "connectDate": "01.12.2016",
 "type": 0,
 "categoryCode": "05",
 "categoryName": "Державна установа",
 "units": [{
    "type": 0,
    "name": "Комплексна інформаційна система",
    "host": " https://kkk.gov.ua",
    "memberId": "1234567891"
 }]
}
```


Ключ	Опис
name	Назва Абонента в Системі BankID НБУ. Може містити літери кирилиці, латиниці, цифри та спеціальні знаки.
edrpou	Код ЄДРПОУ.
connectDate	Дата підключення Абонента до Системи BankID НБУ.
type	Статус Абонента в Системі BankID НБУ: 0 – Абонент-надавач послуг; 1 – Абонент-ідентифікатор; 2 – Абонент-ідентифікатор та Абонент-надавач послуг.
categoryCode	Код категорії Абонента. Складається з цифр. Назва коду категорії в **categoryName.**
categoryName	Назва категорії Абонента. Складається з літер кирилиці.
units	Абонентські вузли Абонента в Системі BankID НБУ.
units.type	Тип абонентського вузла Абонента: 0 – абонентський вузол у статусі Абонента-надавача послуг; 1 – абонентський вузол у статусі Абонента-ідентифікатора.

units.Name	Коротка назва абонентського вузла Абонента в Системі BankID НБУ.
units.memberId	Унікальний ідентифікатор абонентського вузла Абонента в Системі BankID НБУ. Складається із знаків: перші 8 – код ЄДРПОУ; останні 2 – порядковий номер абонентського вузла Абонента.

Інформація для Абонентів-ідентифікаторів, якщо Абонент буде використовувати автентифікацію клієнта за допомогою мобільного застосунку банку, то для коректної ідентифікації у мобільному застосунку “ДІЯ” Державного підприємства “ДІЯ”, необхідно використовувати налаштування відповідно до специфікації https://id.bank.gov.ua/assets/docs/specification_redirect_Diia-2.pdf.

3. Захист інформації в Системі BankID НБУ

3.1. Загальні положення

Передавання інформації між Абонентами Системи BankID НБУ повинна здійснюватися із забезпеченням конфіденційності та контролю цілісності.

Абонентські вузли Абонентів та Центральний вузол забезпечують ідентифікацію та автентифікацію у своїх інформаційно-телекомунікаційних системах із використанням криптографічного протоколу TLS (Transport Layer Security), вимоги до якого наведено нижче.

У абонентських вузлів Абонентів, Центрального вузла здійснюється реєстрація подій шляхом ведення журналу аудиту.

Журнали аудиту повинні бути у текстовому форматі з кодуванням, що підтримують символи кирилиці.

Журнал аудиту абонентського вузла Абонента-надавача послуг повинен містити відомості про факт відправлення електронного запиту на ідентифікацію Центральному вузлу, отримання електронного підтвердження ідентифікації від Центрального вузла, результат розшифрування електронного підтвердження ідентифікації, результат перевірки кваліфікованого електронного підпису/печатки, накладеного Абонентом-ідентифікатором.

Журнал аудиту Абонента-ідентифікатора повинен містити відомості про факт звернення користувача Системи BankID НБУ, результат опрацювання звернення користувача Системи BankID НБУ, факт відправлення електронного підтвердження ідентифікації Центральному вузлу.

Журнал аудиту Центрального вузла повинен містити відомості про факт проходження електронного запиту на ідентифікацію від Абонента-надавача послуг через Центральний вузол до Абонента-ідентифікатора та проходження електронного підтвердження ідентифікації від Абонента-ідентифікатора через Центральний вузол до Абонента-надавача послуг.

Абоненти, адміністратори абонентських вузлів, адміністратори 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 і час події.

Журнали аудиту повинні мати захист від несанкціонованого доступу, модифікації, знищення (руйнування) та зберігатися не менше 90 календарних днів.

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

Абонентські вузли Абонентів та Центральний вузол 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 використовують 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.

Абонентам рекомендується використовувати сертифікати відкритих ключів розширеної перевірки (Extended Validation Certificates, далі – EV SSL сертифікат) у форматі X.509 версії 3 але не нижче OV (Organization Validation).

Рекомендується використовувати браузери 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 перед передаванням електронного підтвердження ідентифікації з інформацією про користувача з використанням Системи 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.

Кваліфікований сертифікат шифрування, який отриманий у будь-якого АЦСК (КНЕДП) України, має бути виданий на ЄДРПОУ установи, з якою укладено договір приєднання до Системи BankID НБУ.

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, коду ЄДРПОУ цього Абонента-ідентифікатора). Абонент-ідентифікатор накладає на електронне підтвердження ідентифікації свою кваліфіковану електронну печатку (кваліфікований електронний підпис — КЕП, Закон України «Про електронні довірчі послуги» https://zakon.rada.gov.ua/laws/show/2155-19#Text) відповідно до вимог «Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час

надання кваліфікованих електронних довірчих послуг», затверджених наказом Міністерства цифрової трансформації України та Адміністрацією державної служби спеціального зв’язку та захисту інформації від 30.09.2020 №140/614 та Вимог.

Шифрування/розшифрування електронного підтвердження ідентифікації відбувається згідно з алгоритмами та правилами, які визначені Вимогами до форматів криптографічних повідомлень.

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, повинен здійснюватися перехід до застосування динамічного механізму узгодження ключів.