Національний банк України
Рада Системи BankID Національного банку України

ЗАТВЕРДЖЕНО
Рішення Ради Системи BankID
Національного банку України
протокол від 20.09.2022
№ В/57-0003/75064 (зі змінами)
(*протоколи від*
09.01.2023 №В/57-0002/3089,
10.05.2024 №В/57-0002/57147,
27.12.2024 №В/57-0002/164776)

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

Версія 2.0

Київ 2024

ЗМІСТ

Глосарій

з/п	Термін, скорочення	Визначення
1	Абонент Системи BankID НБУ (далі – Абонент)	Юридична особа-резидент приватного або публічного права, яка має укладений з Національним банком України (далі – Національний банк) договір приєднання до Системи BankID НБУ (далі – Договір приєднання), та Національний банк.
2	Абонент-надавач послуг	Абонент Системи BankID НБУ, який з її використанням отримує від абонента-ідентифікатора дані користувача Системи BankID НБУ (далі – користувач) з метою надання йому послуг.
3	Абонент-надавач послуг зі спеціальним статусом	Юридична особа з державною формою власності, яка є Абонентом та для забезпечення виконання своїх функцій, передбачених законодавством України, отримує від Абонента-ідентифікатора з використанням Системи BankID НБУ дані користувача та передає їх контрагенту Абонента-надавача послуг зі спеціальним статусом для безпосереднього надання ним послуги цьому користувачу.
4	Абонент-ідентифікатор	Банк України (далі – Банк), який є Абонентом та безпосередньо виконує функції ідентифікації, багатофакторної автентифікації та верифікації клієнтів (Банку), які є користувачами.
5	Абонентський вузол Системи BankID НБУ (далі – абонентський вузол)	Комплекс програмно-технічних засобів, установлений у Абонента та призначений для забезпечення обміну інформацією між Абонентами через Систему BankID НБУ.
6	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.
7	Багатофакторна автентифікація	Це електронна процедура, що дає змогу встановити та підтвердити особу користувача, здійснена із використанням не менше двох факторів автентифікації, кожен із яких має належати до різних категорій факторів автентифікації, а саме – знання, володіння, притаманність.
8	Журнал аудиту	Текстовий файл, в якому реєструються події (запити) та відомості (у вигляді дати, часу, мітки події та описом події) про факт проходження електронного запиту на електронну дистанційну ідентифікацію від Абонента – надавача послуг/Абонента-надавача послуг зі

		спеціальним статусом через Центральний вузол до Абонента–ідентифікатора та про факт проходження електронного підтвердження електронної дистанційної ідентифікації від Абонента-ідентифікатора через Центральний вузол до Абонента – надавача послуг/Абонента-надавача послуг зі спеціальним статусом.
9	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 платіжного застосунку банку з будь-якого пристрою, який має вихід в Інтернет.
10	Електронна дистанційна ідентифікація (далі – ідентифікація)	Процес віддаленого розпізнавання фізичної особи Абонентом-надавачем послуг/контрагентом абонента-надавача послуг зі спеціальним статусом із підтвердженням успішної автентифікації користувача Абонентом-ідентифікатором.
11	Електронний звіт журналу аудиту	Електронний звіт, формується Абонентами та Центральним вузлом у власних інформаційних системах.
12	Кваліфікований сертифікат шифрування	Сертифікат відкритого ключа для шифрування, виданий кваліфікованим надавачем довірчих послуг, перелік яких доступний на вебсайті Центрального засвідчуючого органу Міністерства цифрової трансформації України https://www.czo.gov.ua/ca-registry.
13	Кваліфікований електронний підпис (далі - КЕП)	Відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги» — удосконалений електронний підпис, що створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті електронного підпису.
14	Кваліфікована електронна печатка	Відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги» — удосконалена електронна печатка, що створюється з використанням засобу кваліфікованої електронної печатки і базується на кваліфікованому сертифікаті електронної печатки.
15	Мітка події	Текстова позначка етапу електронного запиту на електронну дистанційну ідентифікацію, визначена у Додатку 3 з ідентифікаторами сесії, призначена для кореляції записів у журналах аудиту абонентських вузлів Абонентів та Центрального вузла.

16	Подія	Відомість/інформація про дію, що ініціюється користувачем/абонентським вузлом/Центральним вузлом на кожному із етапів ідентифікації від електронного запиту на електронну дистанційну ідентифікацію до отримання та розшифрування даних, фіксується Абонентами та Центральним вузлом в журналах аудиту.
17	Портал послуг	Вебсайт (вебпортал), мобільний застосунок (додаток), платіжний застосунок, на якому користувачем ініціюється електронний запит на ідентифікацію.
18	Центральний вузол Системи BankID НБУ (далі – Центральний вузол)	Комплекс програмно-технічних засобів, що забезпечує взаємодію абонентських вузлів.
19	Система BankID НБУ	Національна система електронної дистанційної ідентифікації Національного банку, яка забезпечує здійснення ідентифікації та верифікації фізичних осіб шляхом передавання даних користувачів Абонентом-ідентифікатором Абоненту-надавачу послуг/Абоненту-надавачу послуг зі спеціальним статусом.
20	OAuth 2.0	Відкритий протокол авторизації, який дає змогу третій стороні отримати обмежений доступ до захищених ресурсів користувача без необхідності передавати їй (третій стороні) логін та пароль.

1. Загальна частина

1.1. Призначення документа

Опис функціональних вимог та процесу взаємодії абонентських вузлів, а саме Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом 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 електронними підтвердженнями ідентифікації, що містять зашифровані дані користувача, між абонентськими вузлами через Центральний вузол, який виконує функцію маршрутизатора.

1.3. Концепція функціонування системи

Функціонування Системи BankID НБУ — це взаємодія трьох складових частин:

1. Абонентський вузол Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом;
2. Центральний вузол;
3. Абонентський вузол Абонента-ідентифікатора.

1. **Абонентський вузол Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом —** це комплекс програмно-технічних засобів, на якому розміщені програмні процедури електронного запиту/передачі даних до Центрального вузла на базі протоколу OAuth 2.0.

Електронний запит на ідентифікацію ініціюється користувачем на порталі послуг Абонента-надавача послуг або контрагента Абонента-надавача послуг зі спеціальним статусом (далі – портал послуг), на якому розміщенні форми надання послуг у електронному вигляді. Під час авторизації або замовлення послуги на порталі послуг користувачу доступна можливість авторизації або ідентифікації з використанням Системи BankID НБУ у вигляді кнопки на якій зображено один із логотипів Системи BankID НБУ та яка може мати підпис “Система BankID НБУ”.

Приклад:

“Система BankID НБУ”

Забороняється будь-яким чином змінювати самі логотипи та кольорові гами логотипів (https://bank.gov.ua/admin_uploads/article/Logo_BankID.zip).

Після натискання кнопки з логотипом Системи BankID НБУ користувач з порталу 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. Приклад наведено у п. 2.1.1.

При використанні на своєму порталі послуг способу прямого посилання необхідно відобразити перелік Банків у тій послідовності, як зазначено в переліку Абонентів-ідентифікаторів за посиланням (https://id.bank.gov.ua/api/banks, ключ "order") та забезпечити можливість користувачу вільного вибору Банку. Послідовність Банків визначається на підставі даних статистичної звітності, яка наявна в Національному банку, про загальну кількість клієнтів-фізичних осіб, що мають рахунки в банку від більшого значення до меншого.

Логотипи та/або назви всіх Банків на порталі 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 користувач повинен бути ознайомлений з повним переліком даних, які будуть запитуватися про нього і надати згоду на обробку його даних шляхом проставлення відповідної позначки в явному вигляді відповідно до Закону України “Про захист персональних даних”.

Ознайомлення необхідно реалізувати перед виконанням електронного запиту на ідентифікацію одним із способів:

- розмістити перелік даних, які запитуватимуться через Систему BankID НБУ;
- розмістити посилання (гіперпосилання) на документ, який розміщений на порталі послуг та в якому вказано перелік даних, які запитуватимуться через Систему BankID НБУ для ознайомлення користувачем.

Також, користувач до моменту отримання послуги повинен бути ознайомлений з розміром плати за передавання та/або отримання його даних та надати свою згоду, якщо таку плату встановлено для оплати користувачем.

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 OAuth 2.0.

Після вибору Банку користувач переадресовується на вебадресу 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 було направлено Абонентом-ідентифікатором на його фінансовий номер).

Після успішного проходження процедури багатофакторної автентифікації, користувач переадресовується для отримання послуги на портал послуг, а між Центральним вузлом, абонентським вузлом Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом та абонентським вузлом Абонента-ідентифікатора відбувається автоматична взаємодія шляхом отримання/передачі коду авторизації (**authorization_code**), коду доступу (**access_token**) та 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 OAuth 2.0, автоматичного формування коду авторизації (**authorization_code**), коду доступу (**access_token**), перевірки сертифіката Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом, формування електронної анкети, накладення на неї кваліфікованої електронної печатки Банку, шифрування електронної анкети та переспрямування підписаної і зашифрованої анкети до абонентського вузла Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом через Центральний вузол.

Користувач, якого було переадресовано на вебадресу абонентського вузла Абонента-ідентифікатора має пройти процедуру багатофакторної автентифікації. На цьому абонентському вузлі користувач проходить процедуру багатофакторної 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 ідентифікацію до моменту формування та передачі коду авторизації (**authorization_code**).

Якщо Абонент-ідентифікатор при ідентифікації користувача використовує гіперпосилання (Deep link), яке перенаправляє користувача до платіжного застосунку Банку, то час дії такого гіперпосилання не повинен перевищувати 3 хвилини. Після закінчення визначеного строку дії гіперпосилання (Deep link) воно має стати не активним для користувача, при цьому Абонент-ідентифікатор зобов’язаний проінформувати користувача про це (наприклад: «Час дії сесії сплив. Повторіть спробу або зверніться до Банку», тощо).

У разі успішного проходження багатофакторної автентифікації Абонент-ідентифікатор зобов’язаний проінформувати користувача належним чином про перелік даних, які будуть передані Абоненту–надавачу послуг/Абоненту–надавачу послуг зі спеціальним статусом та отримати від користувача дозвіл на передавання його даних (детальний опис у Додатку 2) .

Після отримання дозволу користувач автоматично переадресовується через Центральний вузол на портал 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 в авторизації, не переспрямовувати неавторизованих клієнтів до Центрального вузла та інформувати клієнта про подальші дії (наприклад: «Перевищено максимальну кількість спроб введення паролю. Повторіть спробу або зверніться до Банку», тощо).

2. Технічна архітектура системи

Взаємодія Центрального вузла з абонентськими вузлами Абонентів (Рис. 1) відбувається на базі протоколу OAuth 2.0 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.

Багатофакторна автентифікація користувача відбувається засобами абонентського вузла Абонента-ідентифікатора. На електронну анкету з даними користувача, що передається, 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/Абонента–надавача послуг зі спеціальним статусом до абонентського вузла Абонента-ідентифікатора через єдиний шлюз, яким виступає Центральний вузол. Усі абонентські вузли Абонентів взаємодіють виключно через Центральний вузол.

Авторизація на базі протоколу 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/Абонента–надавача послуг зі спеціальним статусом з Центральним вузлом

При підключенні до Системи BankID НБУ Абонент-надавач послуг/Абонент–надавач послуг зі спеціальним статусом надає параметр **callback_url** — адреса, на яку буде перенаправлятись запит користувача та в якій буде надаватись код авторизації (**authorization_code**), у випадку успішної багатофакторної автентифікації в Банку. 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/Абонента–надавача послуг зі спеціальним статусом, на яку буде виконано запит з кодом авторизації (**authorization_code**) та здійснена переадресація користувача браузером або іншими засобами для роботи з

	Веб (браузером/Webview) після успішної багатофакторної автентифікації на стороні Банку. Адреса абонентського вузла повинна містити домен порталу послуг цього Абонента-надавача послуг/Абонента– надавача послуг зі спеціальним статусом, який зазначений у рішенні Ради Системи BankID НБУ (якщо інше не вказане в рішенні Ради Системи BankID НБУ).

2.1.1. Запит Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом до Центрального вузла методом GET і отримання коду авторизації (authorization_code) (перший етап)

Запит формується під час переадресації користувача після натискання кнопки на якій зображено логотип Системи BankID НБУ та яка може мати підпис “Система BankID НБУ” на порталі послуг.

Запит повинен містити обов’язкові параметри:

```
https://id.bank.gov.ua/v1/bank/oauth2/authorize
   ?response_type=code
   &client_id=client_id
   &state=state
   &dataset=dataset
```

та, за потреби, додаткові параметри:

```
   &bank_id=name-id
   &lang=en
   &originator_id=12345678
   &originator_url=https://example.gov.ua
```

Приклад структури запиту від абонентського вузла Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом до Центрального вузла:

```
curl -X GET "https://id.bank.gov.ua/v1/bank/oauth2/authorize?
   response_type=code&
   client_id=client_id&
   state=state&
   dataset=11"
```

Відповідь Центрального вузла:

```
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/Абонента–надавача послуг зі спеціальним статусом і буде повернуто Центральним вузлом в запиті з кодом авторизації (**authorization_code**). Не більше 50 знаків.
dataset	Номер стандартизованого набору даних, який відповідає тому переліку ключів, які необхідно запитати абонентському вузлу Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом у Абонента-ідентифікатора та на який Абонент-надавач послуг/Абонент–надавач послуг зі спеціальним статусом має відповідний дозвіл Ради Системи BankID. Перелік стандартизованих наборів даних вказано у Додатку 1.
bank_id	Ідентифікатор абонентського вузла Абонента-ідентифікатора. Параметр обов’язковий у випадку якщо Абонент-ідентифікатор обирається безпосередньо на порталі послуг. Значення має бути обрано із ключа «**id**» (детальний опис у п. 2.4.). В інших випадках цей параметр необов’язковий.
originator_id	Унікальний ідентифікаційний номер контрагента Абонента–надавача послуг зі спеціальним статусом в Єдиному державному реєстрі підприємств та організацій України (код ЄДРПОУ), яка ініціює запит на інформацію. Не більше 8 цифр. Параметр обов’язковий до заповнення для абонентського

	вузла Абонента–надавача послуг зі спеціальним статусом до якого підключено більше одного контрагента (наприклад, “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). Параметр обов’язковий до заповнення для абонентського вузла Абонента-надавача послуг та Абонента–надавача послуг зі спеціальним статусом до якого підключено більше одного контрагента (наприклад, “Інтегрована система електронної ідентифікації – ID.GOV.UA”).
lang	Мовний показник. Може мати значення “en” – англомовний текст. Параметр необов’язковий, використовується абонентським вузлом Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом у випадку якщо користувач обирає безпосередньо на його порталі послуг англомовний вебінтерфейс з метою подальшого спрямування цього користувача на англомовну версію форми авторизації на стороні Абонента-ідентифікатора. Якщо з боку абонентського вузла Абонента-ідентифікатора немає підтримки мовних версій, форма авторизації користувача, по замовчуванню, матиме виключно україномовний текст.

У разі успішної багатофакторної автентифікації користувача Абонентом-ідентифікатором, Абонент-ідентифікатор виконує запит з кодом авторизації (**authorization_code)** та переадресовує користувача з абонентського вузла до Центрального вузла, а Центральний вузол у свою чергу виконує **GET**-запит та переадресацію запиту користувача до абонентського вузла Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом із кодом авторизації (**authorization_code)** на зареєстрований параметр **callback_url**.

Приклад структури запиту (переадресації) з кодом авторизації (**authorization_code**) від Центрального вузла до абонентського вузла Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом:

```
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. Не більше 50 знаків.
state	Значення параметра, яке передав абонентський вузол Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом у першому GET запиті до Центрального вузла.

Можливі помилки

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

- абонентський вузол Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом не вдалося ідентифікувати, зокрема, абонентський вузол не зареєстрований на стороні Центрального вузла, або некоректно передано параметр та/або його значення 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. У такому випадку причина помилки має відображатися користувачу на стороні Абонента-ідентифікатора.

2.1.2. Запит Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом до Центрального вузла на отримання коду доступу (access_token) методом POST (другий етап)

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

Приклад структури запиту від абонентського вузла Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом 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/Абонента–надавача послуг зі спеціальним статусом, 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. Не більше 50 знаків.
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 OAuth 2.0 (https://tools.ietf.org/html/rfc6749#section-5.2). Зокрема: **invalid_client** – у запиті некоректно вказані ідентифікатори абонентського вузла Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом (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; **repeat_request** – повторний запит на код доступу (**access_token**); **server_error** – запит по вказаному коду авторизації не знайдено або 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.

2.2. 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 багатофакторної 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 даних користувача.

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

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

Запит повинен містити обов'язкові параметри:

```
https://id.bank.gov.ua/v1/bank/oauth2/authorize
   ?response_type=code
   &client_id=client_id
   &state=state
   &dataset=11
   &units_name=units_name
```

та, за потреби, додаткові параметри:

```
   &lang=en
```

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&
    dataset=11&
    units_name=units_name"
```

Відповідь Абонента-ідентифікатора:

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

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 (**authorization_code**). Не більше 50 знаків.
dataset	Номер стандартизованого набору даних, який відповідає тому переліку ключів, які необхідно запитати абонентському вузлу Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом у Абонента-ідентифікатора та на який Абонент-надавач послуг/Абонент –надавач послуг зі спеціальним статусом має відповідний дозвіл Ради Системи BankID. Перелік стандартизованих наборів даних вказано у Додатку 1.
units_name	Назва абонентського вузла Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом від якого було ініційовано запит та яка відповідає назві, що вказана у рішенні Ради Системи BankID НБУ. Параметр додається Центральним вузлом. Текст кириличними символами кодується за допомогою методу encodeURI у форматі UTF-8. Абонент-ідентифікатор повинен опрацювати (декодувати) даний текст і повідомити (відобразити) назву абонентського вузла Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом від якого було ініційовано ідентифікацію користувачу на стороні вебсторінки/платіжного застосунку Банку (приклад наведено у Додатку 2).
lang	Мовний показник. Може мати значення “en” – англомовний текст. Параметр необов’язковий, використовується абонентським вузлом Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом у випадку якщо користувач обирає безпосередньо на його порталі послуг англомовний вебінтерфейс з метою подальшого спрямування цього

	користувача на англомовну версію форми авторизації на стороні Абонента-ідентифікатора. Якщо з боку абонентського вузла Абонента-ідентифікатора немає підтримки мовних версій, форма авторизації користувача, по замовчуванню, матиме виключно україномовний текст.

У разі успішної багатофакторної автентифікації користувача Абонентом-ідентифікатором абонентський вузол Абонента-ідентифікатора здійснює переадресацію користувача до Центрального вузла із кодом авторизації (**authorization_code)** на параметр **callback_url**.

Приклад структури запиту з кодом авторизації (**authorization_code**) 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 після успішної багатофакторної автентифікації здійснюватиме переадресацію користувача із кодом авторизації (**authorization_code**).
code	Код авторизації (**authorization_code**) — унікальний ідентифікатор, який формується на стороні вузла Абонента-ідентифікатора. Час дії коду 90 секунд. Не більше 50 знаків.
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 Центрального вузла 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": 120
}
```

Параметр	Опис
token_type	Значення повинно бути **“bearer”**.

access_token	Значення коду доступу. Не більше 50 знаків.
expires_in	Термін дії коду доступу (значення в секундах). Повинен мати значення 120.

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 OAuth 2.0 (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; **repeat_request** – повторний запит на код доступу (**access_token**); **server_error** – запит по вказаному коду авторизації не знайдено або 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

Для отримання даних користувача абонентський вузол Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом здійснює запит на дані до Центрального вузла (п. 2.3.1.). Центральний вузол здійснює запит на вебадресу (**data_api_url** п. 2.2.) абонентського вузла Абонента-ідентифікатора (п. 2.3.2.). Надання даних користувача відбувається на підставі коду доступу (**access_token**) та кваліфікованого сертифікату шифрування (**cert**).

Код доступу передається в заголовку (**headers**) запиту на дані у вигляді:

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

Сертифікат шифрування Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом передається в тілі запиту (body) у значенні ключа "**cert**".

Значення/Ключ	Опис
access_token	Отримане значення коду доступу (п. 2.1.2. та п. 2.2.2.).
cert	Ключ у значенні якого передається кваліфікований сертифікат шифрування Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом. Передається у форматі DER закодованого в BASE64.

2.3.1. Запит на дані від абонентського вузла Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом

Перелік необхідних ключів (даних) по користувачу формується Центральним вузлом, у відповідності до значення параметра **dataset**, при отриманні першого **GET**-запиту (п. 2.1.1.). Отже, абонентський вузол Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом повинен передати в тілі запиту на дані тільки кваліфікований сертифікат шифрування.

Приклад запиту на дані:

```
curl -X POST https://id.bank.gov.ua/v1/bank/resource/client
  -H "Content-Type: application/json" -H "Authorization: Bearer access_token"
  -d '{ "cert":"Encode to base64 format" }'
```

2.3.2. Запит на дані до абонентського вузла Абонента-ідентифікатора

Запит на дані від абонентського вузла Абонента-надавача послуг/ Абонента–надавача послуг зі спеціальним статусом буде доповнено Центральним вузлом переліком ключів, які відповідають обраному номеру набору даних відповідно до номеру стандартизованого набору (**dataset**), що було вказано в **GET-**запиті (п. 2.1.1.), ключами і значеннями **memberId**, **sidBi** та буде направлено до абонентського вузла Абонента-ідентифікатора.

Термін очікування відповіді Центральним вузлом від Абонента-ідентифікатора на запит даних становитиме 30 секунд.

Приклад запиту на дані до Абонента-ідентифікатора:

```
curl -X POST https://example.bank.com.ua/v1/bank/data
  -H "Content-Type: application/json" -H "Authorization: Bearer access_token"
  -d '{"type": "physical",
        "cert": "Encode to base64 format",
        "sidBi": "some-session-guid",
        "memberId": "0212345678",
        "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":[
              " "series", "number",
              "issue", "dateIssue", "issueCountryIso2"
           ]}
        ]
}'
```

2.3.3. Вимоги щодо передачі Абонентом-ідентифікатором 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 містяться в електронному запиті на ідентифікацію Абонента-надавача послуг.

Якщо дані клієнта за обов’язковими ключам відсутні в 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 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. Абонент-ідентифікатор зобов’язаний здійснювати процедуру актуалізації даних про клієнтів у порядку та строки, які встановлені законодавством з питань фінансового моніторингу. У разі необхідності здійснення актуалізації даних, 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 ідентифікації вважається таким, що не відповідає вимогам цієї специфікації і може бути оскаржене Абонентом-надавачем послуг/Абонентом-надавачем послуг зі спеціальним статусом та визнане таким, що не підлягає тарифікації за міжабонентськими тарифами.

(вимоги першого речення цього абзацу не застосовуються до абонентів-ідентифікаторів Системи BankID НБУ протягом дії воєнного стану в Україні, рішення Ради Системи BankID НБУ від 26.09.2022 № В/57-0003/76967, зі змінами)

Дані клієнта за ключами, які не позначені в цій специфікації як обов’язкові до заповнення, за наявності, передаються Абонентом-ідентифікатором, але не є предметом оскарження.

Якщо у складі обраного Абонентом-надавачем послуг/Абонентом–надавачем послуг зі спеціальним статусом номері стандартизованого набору є 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 (зразка 1994 року) ("passport"), паспорт громадянина України (ID-картка) ("IDcard"), паспорт громадянина України для виїзду за кордон ("ipassport"), інший документ, що посвідчує особу та відповідно до законодавства України може бути використаний на території України для укладення правочинів, в тому числі і національний паспорт іноземця або документ, що його замінює ("ident"). Інформація надана Абонентом-ідентифікатором у відповідності до цих вимог, вважається такою, що надана в 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 ідентифікації вважається таким, що не відповідає вимогам цієї специфікації і може бути оскаржене Абонентом-надавачем послуг/Абонентом–надавачем послуг зі спеціальним статусом та визнане таким, що не підлягає тарифікації за міжабонентськими тарифами.

Абоненту-ідентифікатору забороняється передавати дані за запитом Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом 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/Абонента-надавача послуг зі спеціальним статусом (не застосовується до типу документа "passport"). Невиконання цієї умови Абонентом-ідентифікатором є порушенням вимог цієї специфікації.

(вимоги цього абзацу не застосовуються до абонентів-ідентифікаторів Системи BankID НБУ протягом дії воєнного стану в Україні, рішення Ради Системи BankID НБУ від 26.09.2022 № В/57-0003/76967, зі змінами)

Якщо у складі обраного Абонентом-надавачем послуг/Абонентом–надавачем послуг зі спеціальним статусом номері стандартизованого набору є ключ "phone", Абонент-ідентифікатор зобов’язаний передати коректний номер(и) контактного телефону клієнта, що використовується банком, зокрема, з метою проведення його автентифікації. Якщо відповідь Абонента-ідентифікатора за ключем "phone" містить не коректний номер(и) контактного телефону клієнта, то таке електронне підтвердження ідентифікації вважається таким, що не відповідає вимогам цієї специфікації і може бути оскаржене Абонентом-надавачем послуг/Абонента-надавача послуг зі спеціальним статусом та визнане таким, що не підлягає тарифікації за міжабонентськими тарифами.

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

Якщо у складі обраного Абонентом-надавачем послуг/Абонентом-надавачем послуг зі спеціальним статусом номері стандартизованого набору є ключ "addresses", Абонент-ідентифікатор зобов’язаний передати дані не менше ніж за одним типом адреси: фактична адреса (місце перебування) та/або адреса реєстрації (місце проживання)). Якщо у відповіді Абонента-ідентифікатора надано інформацію за одним типом адреси, то така інформація є наданою в повному обсязі та не може бути оскаржена Абонентом-надавачем послуг/Абонента–надавача послуг зі спеціальним статусом.

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

Абонент-ідентифікатор та Абонент-надавач послуг, який є комерційним Абонентом, зобов’язані забезпечити зберігання в електронному вигляді не менше п’яти років після припинення ділових відносин із користувачем або завершення разової операції/надання послуги без встановлення ділових відносин із користувачем, щодо якого абонентом було отримане або надане електронне підтвердження ідентифікації, для можливості вирішення спорів між абонентами та/або абонентом та користувачем щодо успішних електронних підтверджень ідентифікації:

1) електронний запит на ідентифікацію та електронне підтвердження ідентифікації користувача, здійснених із використанням Системи BankID НБУ;

2) інформації (технічних параметрів, які дають змогу ідентифікувати електронний запит на ідентифікацію/електронне підтвердження ідентифікації та факт їх проходження між суб’єктами) про передавання до та отримання від Центрального вузла Системи BankID НБУ електронного запиту на ідентифікацію та електронного підтвердження ідентифікації.

Абонент-надавач послуг зі спеціальним статусом та некомерційний Абонент-надавач послуг зобов’язані забезпечити зберігання в електронному вигляді значень таких ключів Електронної анкети (Додаток 1), як ідентифікатор сесії та унікальний ідентифікатор абонентського вузла в Системі BankID НБУ, та іншої інформації (технічних параметрів, які дають змогу ідентифікувати електронний запит на ідентифікацію/електронне підтвердження ідентифікації та факт їх проходження міжсуб’єктами) не менше п’яти років із дати ініціювання електронного запиту на ідентифікацію/надходження електронного підтвердження ідентифікації, про:

1) передавання електронного запиту на ідентифікацію до та отримання електронного підтвердження ідентифікації від Центрального вузла Системи BankID НБУ;

2) отримання електронного запиту на ідентифікацію від та передавання електронного підтвердження ідентифікації до контрагентів Абонента-надавача послуг зі спеціальним статусом (для Абонентів-надавачів послуг зі спеціальним статусом).

2.3.4. Відповідь з даними користувача

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 (значення помилки “**invalid_edrpou**” — детальніше у прикладах можливих помилок).

Дані Абонент-ідентифікатор формує в 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",
   "flagPEP": "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",
      "паспорт громадянина України (зразка 1994 року).",
      "series": "AA",
      "number": "222333",
      "issue": "Ківерцівським РО УМВД",
      "dateIssue": "15.03.1999"

   }]
}
```

Вказаний Json-об’єкт підписується кваліфікованою електронною печаткою Абонента-ідентифікатора і шифрується за алгоритмом визначеним у ДСТУ ГОСТ 28147-2009. Шифрування підписаних 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 Json-об’єкта в значенні ключа "**customerCrypto**".

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)"
}
```

Ключ	Опис
cert	Кваліфікований сертифікат шифрування Абонента-ідентифікатора. Передається у форматі DER закодованого в BASE64.
customerCrypto	Цифровий конверт, що містить зашифровані дані користувача, на які накладено кваліфіковану електронну печатку Банку та закодовано в BASE64.

Отримана відповідь від абонентського вузла Абонента-ідентифікатора доповнюється Центральним вузлом ключами/значеннями **memberId**, **sidBi** і

перенаправляється абонентському вузлу Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом.

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"
}
```

Ключ	Опис
error	Помилки, що визначаються Абонентами-ідентифікаторами: **invalid_request** – у запиті на отримання 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 або недійсний сертифікат, що був наданий абонентським вузлом Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом; **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 при обробці Банком запиту на дані; **invalid_edrpou** – код ЄДРПОУ отримувача даних (отримано із сертифікату запиту на дані) не відповідає унікальному ідентифікатору абонентського вузла

	Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом (значення ключа **memberId**). Помилки, що визначаються Центральним вузлом: **invalid_request** – некоректний запит на дані; **invalid_token** – відсутній або невірно зазначений код доступу (**access_token**) або термін дії коду доступу завершився; **repeat_request** – вузлом Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом здійснено повторний запит на отримання даних; **request_timeout** – термін відповіді Абонента-ідентифікатора на запит даних завершився; **invalid_response** – у відповіді Абонента-ідентифікатора на запит даних некоректно зазначений параметр (ключ **error** або **error_description**) помилки або немає тіла (body) або тіло відповіді не у Json-форматі; **invalid_server –** помилка при обробці центральним вузлом запиту на дані.
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**»; «Помилка при перевірці коду ЄДРПОУ запитувача. Помилка: код ЄДРПОУ запитувача не відповідає коду абонентського вузла Абонента-надавача послуг/Абонента –надавача послуг зі спеціальним статусом».
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, у тому числі в запиті з кодом авторизації (**authorization_code**)) 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 абонентських вузлів Абонентів-ідентифікаторів у Системі BankID НБУ

Посилання на перелік абонентських вузлів Абонентів-ідентифікаторів (у Json-форматі): https://id.bank.gov.ua/api/banks.

Приклад структури по одному із вузлів Абонента-ідентифікатора:


```
{
  "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 до конкретного Банку, 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 у Системі BankID НБУ

Посилання на перелік Абонентів (у Json-форматі): https://id.bank.gov.ua/v1/api/abonents.

Приклад запиту по значенню ЄДРПОУ Абонента, наприклад: https://id.bank.gov.ua/v1/api/abonents/?edrpou=37508596.

Приклад запиту по значенню “memberId”:– https://id.bank.gov.ua/v1/api/abonents/3750859601.

Приклад відповіді по одному 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/Абонент–надавач послуг зі спеціальним статусом; 1 – Абонент-ідентифікатор; 2 – Абонент-ідентифікатор та/або Абонент-надавач послуг/Абонент–надавач послуг зі спеціальним статусом.
categoryCode	Код категорії Абонента. Складається з цифр. Назва коду категорії в **categoryName.**
categoryName	Назва категорії Абонента. Складається з літер кирилиці.
disabledType	Роботу абонента в Системі BankID НБУ тимчасово зупинено у статусі: 0 – Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом; 1 – Абонента-ідентифікатора; 2 – Абонента-ідентифікатора та/або Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом.
units	Абонентські вузли Абонента в Системі BankID НБУ.
units.type	Тип абонентського вузла Абонента: 0 – абонентський вузол у статусі Абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом; 1 – абонентський вузол у статусі Абонента-ідентифікатора.
units.name	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 багатофакторну автентифікацію клієнта за допомогою мобільного застосунку банку, то для коректної ідентифікації в 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 та вимоги до журналів аудиту

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

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

У абонентських вузлів Абонентів та Центрального вузла здійснюється реєстрація подій шляхом формування:

- журналів аудиту в текстовому форматі з кодуванням, що підтримують символи кирилиці;

- електронних звітів журналів аудиту згідно з Додатком 4, з можливістю виконання витягів за необхідний період.

Усі записи в журналах аудиту повинні містити дату, час події і мітку події. Мітку події потрібно записувати перед записом самої події.

Мітка події складається з префікса «**MARK**», ідентифікатора події, ідентифікаторів сесії **sidBi** і **state**, які розділяються дефісом.

Ідентифікатор сесії **sidBi** – зазначається в усіх мітках подій абонентським вузлом Абонентом-ідентифікатором та Центральним вузлом. Абонентом-надавачем послуг/Абонентом-надавачем послуг зі спеціальним статусом зазначається у мітці події **ResponsPOST13** після отримання ідентифікатора в електронному підтвердженні ідентифікації.

Ідентифікатор сесії **state** – зазначається у всіх мітках подій абонентськими вузлами Абонентами-надавачами послуг/Абонентами-надавачами послуг зі спеціальним статусом та у мітці події GET1 Центральним вузлом.

Приклади міток подій:

• MARK - GET1 - sidBi=f0db3653-c0b2-4970-aa32-c599d02462e1 (журнал аудиту абонентського вузла Абонента-ідентифікатора);

• MARK - GET1 - state=dfad23a3e38023526d76bbae40ade73c576afb09 (журнал аудиту абонентського вузла Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом);

• MARK - ResponsPOST13 - sidBi=f0db3653-c0b2-4970-aa32-c599d02462e1 - state=dfad23a3e38023526d76bbae40ade73c576afb09 (журнал аудиту абонентського вузла Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом);

• MARK - GET1 - sidBi=f0db3653-c0b2-4970-aa32-c599d02462e1 - state=dfad23a3e38023526d76bbae40ade73c576afb09 (журнал аудиту Центрального вузла).

Журнал аудиту абонентського вузла Абонента-надавача послуг/Абонента -надавача послуг зі спеціальним статусом повинен містити відомості про факти подій:

- 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 абонентського вузла Абонента-ідентифікатора повинен містити відомості про факти подій:

- 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 факти подій:

- проходження електронного запиту на ідентифікацію від Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом через Центральний вузол до Абонента-ідентифікатора та проходження електронного підтвердження ідентифікації від Абонента-ідентифікатора через Центральний вузол до Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом.

В журналі аудиту абонентський вузол Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом та абонентський вузол Абонента-ідентифікатора зобов’язані записувати мітки подій згідно ідентифікаторів подій, які вказані у Додатку 3. Абоненти, адміністратори абонентських вузлів, адміністратори Системи BankID НБУ мають право самостійно визначати додаткові події, що фіксуються у відповідних журналах аудиту.

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/Абонента–надавача послуг зі спеціальним статусом, 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 електронну ідентифікацію та 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.

Додаток 1
до Специфікації взаємодії абонентського
вузла з центральним вузлом Системи BankID
Національного банку України

Електронна анкета (з переліком та описом допустимих ключів) та стандартизовані набори даних

Електронна анкета					**Стандартизовані набори даних (параметр dataset)**												
Ключ			**Значення ** (формат та вимоги)**	**Опис**	**11**	**12**	**13**	**21**	**22**	**23**	**31**	**32**	**41**	**42**	**51**	**61**	**71**
cert*			Формат сертифікату DER, закодовано за стандартом BASE64.	Кваліфікований сертифікат шифрування.	Технічний блок ключів												
memberId			XXXXXXXXNN – де: XXXXXXXX – ідентифікатор абонента (код ЄДРПОУ); NN – порядковий номер абонентського вузла. Ключ та значення додаються Центральним вузлом.	Унікальний ідентифікатор абонентського вузла Абонента в Системі BankID НБУ.													
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	▪	▪	▪	▪	▪	▪	▪	▪	▪	▪	▪	▪	▪

Електронна анкета					Стандартизовані набори даних (параметр dataset)												
Ключ			Значення ** (формат та вимоги)	Опис	11	12	13	21	22	23	31	32	41	42	51	61	71
		middleName*	У разі відсутності по батькові у документах користувача, необхідно передавати значення «**n/a**»***. Можливі значення: 'по батькові' або 'n/a'.	По батькові	▪	▪	▪	▪	▪	▪	▪	▪	▪	▪	▪	▪	▪
		phone*	Номер телефону може мати тільки цифрове значення та відповідати формату CCNDCSN, де CC – код країни, NDC - національний код призначення, SN - номер користувача. Якщо у користувача декілька номерів контактного телефону, то значення розділяються знаком коми «,». Наприклад: 380501234567, 380971234567	Номер (и) контактного телефону				▪	▪	▪			▪	▪		▪	▪
		inn*	Можливі значення: 'XXXXXXXXXX' – РНОКПП, де X може мати лише цифрове значення; 'NNXXXXXX' - паспорт, де NN – серія, XXXXXX – цифрове значення номеру паспорта; 'XXXXXXXXX' – номер id картки, де X може мати лише цифрове значення;	Для резидента - реєстраційний номер облікової картки платника податків або номер (та за наявності - серія) паспорта, в якому проставлено відмітку про відмову від прийняття реєстраційного номера облікової картки платника податків або номер паспорта із записом про відмову від прийняття реєстраційного номера облікової картки платника податків в			▪			▪	▪	▪	▪	▪	▪	▪	▪

Електронна анкета					Стандартизовані набори даних (параметр dataset)												
Ключ			Значення ** (формат та вимоги)	Опис	11	12	13	21	22	23	31	32	41	42	51	61	71
			або 'n/a'.	електронному безконтактному носії. Для нерезидента – реєстраційний номер облікової картки платника податків або 'n/a'													
		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													▪
		dateOfBirth*	dd.mm.yyyy	Дата народження								▪		▪	▪	▪	▪
		placeOfBirth*	Якщо документ особи не передбачає наявності відомостей про місце народження, необхідно передавати значення 'n/a'. Можливі значення: 'місце народження' або 'n/a'.	Місце народження (за наявності)											▪	▪	▪
		nationality*	Можливі значення: 'UA'/ 'UKR' або інший літерний код країни за стандартом ISO_3166-1 (alfa-2/alfa-3) або 'n/a'.	Громадянство нерезидента (для резидентів заповнюється за наявності)								▪		▪	▪	▪	▪
		sex*	Можливі значення: латинська літера M – чоловіча або F – жіноча	Стать								▪		▪	▪	▪	▪

Електронна анкета					Стандартизовані набори даних (параметр dataset)												
Ключ			Значення ** (формат та вимоги)	Опис	11	12	13	21	22	23	31	32	41	42	51	61	71
		email*	Якщо у користувача відсутня адреса електронної пошти, необхідно передавати значення 'n/a'. Можливі значення: 'адреса електронної пошти' або 'n/a'.	Адреса електронної пошти (за наявності)				▪	▪	▪			▪	▪		▪	▪
		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 PEP (публічно значущі особи, члени сім’ї, пов’язані) відповідно до законодавства													▪
		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													▪

Електронна анкета					Стандартизовані набори даних (параметр dataset)												
Ключ			Значення ** (формат та вимоги)	Опис	11	12	13	21	22	23	31	32	41	42	51	61	71
				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 високий (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													▪
		phoneNumberChange	dd.mm.yyyy	Дата встановлення або дата зміни фінансового номеру телефону в системах Абонента-ідентифікатора													▪
		identificationDate*	dd.mm.yyyy	Дата проходження ідентифікації/переідентифікації(з перевіркою ідентифікаційного документу) особою													▪
		clarificationDate	dd.mm.yyyy	Дата останнього уточнення інформації про особу													▪
addresses	**Масив типів адрес та адресних даних особи**				▪			▪							▪	▪	▪

Електронна анкета					Стандартизовані набори даних (параметр dataset)												
Ключ			Значення ** (формат та вимоги)	Опис	11	12	13	21	22	23	31	32	41	42	51	61	71
	type*		Можливі значення: **factual.**	Тип адреси проживання: factual – фактична адреса проживання (місце перебування).	▪			▪							▪	▪	▪
	fields		**Масив адресних даних особи**		▪			▪							▪	▪	▪
		country*	Можливі значення: 'UA'/ 'UKR' або інший літерний код країни за стандартом ISO_3166-1 (alfa-2/alfa-3).	Країна проживання	▪			▪							▪	▪	▪
		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	Тип вулиці (наприклад: вулиця, узвіз, проспект і тд) та її назва	▪			▪							▪	▪	▪

Електронна анкета					Стандартизовані набори даних (параметр dataset)												
Ключ			**Значення ** (формат та вимоги)**	**Опис**	**11**	**12**	**13**	**21**	**22**	**23**	**31**	**32**	**41**	**42**	**51**	**61**	**71**
			значення: 'тип вулиці та її назва' або 'n/a'.														
		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)	▪			▪							▪	▪	▪
	type*		Можливі значення: **juridical.**	Тип адреси проживання: juridical – адреса реєстрації (місце проживання)	▪			▪							▪	▪	▪
	fields		**Масив адресних даних особи**		▪			▪							▪	▪	▪
		country*	Можливі значення: 'UA'/ 'UKR' або інший літерний код країни за стандартом ISO_3166-1 (alfa-2/alfa-3).	Країна 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	Район	▪			▪							▪	▪	▪

Електронна анкета					Стандартизовані набори даних (параметр dataset)												
Ключ			Значення ** (формат та вимоги)	Опис	11	12	13	21	22	23	31	32	41	42	51	61	71
			району, необхідно передавати значення 'n/a'. Можливі значення: 'назва району' або 'n/a'.														
		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**					▪			▪		▪		▪		▪	▪	▪

Електронна анкета					Стандартизовані набори даних (параметр dataset)												
Ключ			**Значення ** (формат та вимоги)**	**Опис**	**11**	**12**	**13**	**21**	**22**	**23**	**31**	**32**	**41**	**42**	**51**	**61**	**71**
	type*		Можливі значення: **passport**	Тип документу: **passport** – паспорт громадянина України (зразка 1994 року)		▪			▪		▪		▪		▪	▪	▪
	fields	**Масив реквізитів документу, що посвідчують особу**				▪			▪		▪		▪		▪	▪	▪
		series*****	Можливі значення: 'NN', де N – може мати тільки латинські літери .	Серія документа		▪			▪		▪		▪		▪	▪	▪
		number*****	Можливі значення: XXXXXX, де X – може мати тільки цифрове значення.	Номер документа		▪			▪		▪		▪		▪	▪	▪
		issue*****		Орган, що видав документ							▪		▪		▪	▪	▪
		dateIssue*****	dd.mm.yyyy	Дата видачі документу							▪		▪		▪	▪	▪
		issueCountryIso2	Можливі значення: 'UA'/ 'UKR' або інший літерний код країни за стандартом ISO_3166-1 (alfa-2/alfa-3).	Країна видачі документа							▪		▪		▪	▪	▪
	type*		Можливі значення: **IDcard**	Тип документу: **IDcard** – паспорт громадянина України (ID-картка)		▪			▪		▪		▪		▪	▪	▪
	fields	**Масив реквізитів документу, що посвідчують особу**				▪			▪		▪		▪		▪	▪	▪
		number*****	Можливі значення:	Номер документа		▪			▪		▪		▪		▪	▪	▪

Електронна анкета					Стандартизовані набори даних (параметр dataset)												
Ключ			Значення ** (формат та вимоги)	Опис	11	12	13	21	22	23	31	32	41	42	51	61	71
			XXXXXXXXX, де X – може мати тільки цифрове значення														
		issue*	Можливі значення: XXXX, де X – може мати тільки цифрове значення	Орган, що видав документ							▪		▪		▪	▪	▪
		dateIssue*	dd.mm.yyyy	Дата видачі документу							▪		▪		▪	▪	▪
		dateExpiration*	Можливі значення: 'dd.mm.yyyy'	Дата закінчення строку дії							▪		▪		▪	▪	
		recordEDDR*	Можливі значення: 'XXXXXXXX-XXXXX' – де X може приймати лише цифрове значення	Унікальний номер запису в Єдиному державному демографічному реєстрі							▪		▪		▪	▪	▪
		issueCountryIso2	Можливі значення: 'UA'/ 'UKR' або інший літерний код країни за стандартом ISO_3166-1 (alfa-2/alfa-3).	Країна видачі документа							▪		▪		▪	▪	▪
	type*		Можливі значення: **ipassport**	Тип документу: **ipassport** – паспорт громадянина України для виїзду за кордон		▪			▪		▪		▪		▪	▪	▪
	fields	**Масив реквізитів документу, що посвідчують особу**				▪			▪		▪		▪		▪	▪	▪
		series*	Можливі значення: 'NN', де N – може мати тільки латинські літери	Серія документа		▪			▪		▪		▪		▪	▪	▪
		number*	Можливі значення: XXXXXXXXX, де X – може мати тільки цифрове значення.	Номер документа		▪			▪		▪		▪		▪	▪	▪
		issue*	Можливі значення: XXXX, де X – може мати тільки цифрове значення	Орган, що видав документ							▪		▪		▪	▪	▪
		dateIssue*	dd.mm.yyyy	Дата видачі документу							▪		▪		▪	▪	▪

Електронна анкета					Стандартизовані набори даних (параметр dataset)												
Ключ			**Значення ** (формат та вимоги)**	**Опис**	**11**	**12**	**13**	**21**	**22**	**23**	**31**	**32**	**41**	**42**	**51**	**61**	**71**
		dateExpiration*****	Можливі значення: 'dd.mm.yyyy'	Дата закінчення строку дії							▪		▪		▪	▪	▪
		recordEDDR*****	Заповнюється відповідно до вимог законодавства України. Можливі значення: 'XXXXXXXX-XXXXX' – код, де X може приймати лише цифрове значення	Унікальний номер запису в Єдиному державному демографічному реєстрі							▪		▪		▪	▪	▪
		issueCountryIso2	Можливі значення: 'UA'/ 'UKR' або інший літерний код країни за стандартом ISO_3166-1 (alfa-2/alfa-3).	Країна видачі документа							▪		▪		▪	▪	▪
	type*		Можливі значення: **ident**	Тип документу: **ident** – інший документ, що посвідчує особу та відповідно до законодавства України може бути використаний на території України для укладення правочинів, в тому числі і національний паспорт іноземця або документ, що його замінює		▪			▪		▪		▪		▪	▪	▪
	fields	**Масив реквізитів документу, що посвідчують особу**				▪			▪		▪		▪		▪	▪	▪
		series*****	Можливі значення: 'серія' або 'n/a'.	Серія документа (для осіб - нерезидентів заповнюється за наявності серії в їх документах). Якщо документ особи не передбачає наявності серії документу, необхідно передавати значення 'n/a'		▪			▪		▪		▪		▪	▪	▪
		number*****		Номер документа		▪			▪		▪		▪		▪	▪	▪

Електронна анкета					Стандартизовані набори даних (параметр dataset)												
Ключ			Значення ** (формат та вимоги)	Опис	11	12	13	21	22	23	31	32	41	42	51	61	71
		issue*		Яким органом видано документ							▪		▪		▪	▪	▪
		dateIssue*	dd.mm.yyyy	Дата видачі документу							▪		▪		▪	▪	▪
		dateExpiration*	Якщо документ особи не передбачає наявності дати закінчення строку дії, необхідно передавати значення 'n/a'. Можливі значення: 'dd.mm.yyyy' або 'n/a'	Дата закінчення строку дії							▪		▪		▪	▪	▪
		recordEDDR*	Заповнюється відповідно до вимог законодавства України. Якщо документ особи не передбачає наявності Унікального номеру запису в Єдиному державному демографічному реєстрі, необхідно передавати значення 'n/a'. Можливі значення: 'XXXXXXXX-XXXXX' – код, де X може приймати лише цифрове значення або 'n/a'	Унікальний номер запису в Єдиному державному демографічному реєстрі (заповнюється за наявності інформації у документах особи)							▪		▪		▪	▪	▪
		issueCountryIso2	Можливі значення: 'UA'/ 'UKR' або інший літерний код країни за стандартом ISO_3166-1 (alfa-2/alfa-3).	Країна видачі документа							▪		▪		▪	▪	▪

* — обов’язкові ключі для заповнення Абонентом-ідентифікатором.

** — всі значення ключів мають символьний тип.

*** — у Системі BankID НБУ скорочення 'n/a' використовується в значенні не застосовується (англ. not applicable).

Додаток 2
до Специфікації взаємодії абонентського
вузла з центральним вузлом Системи BankID
Національного банку України

Опис даних стандартизованих наборів (dataset)

З метою інформування користувача про перелік даних, які будуть передані Абоненту-надавачу послуг/Абонент-надавачу послуг зі спеціальним статусом Абонент-ідентифікатор після отримання в електронному запиті на ідентифікацію (п.2.2.1) номеру стандартизованого набору даних використовує інформацію, що наведена у таблиці:

Номер стандартизованого набору даних	Інформація для користувача
11	Прізвище, Ім’я, По батькові, Дані щодо місця перебування або проживання
12	Прізвище, Ім’я, По батькові, Дані ідентифікаційного документу
13	Прізвище, Ім’я, По батькові, РНОКПП
21	Прізвище, Ім’я, По батькові, Дані щодо місця перебування або проживання Номер контактного телефону, Адреса електронної пошти
22	Прізвище, Ім’я, По батькові, Дані ідентифікаційного документу, Номер контактного телефону, Адреса електронної пошти
23	Прізвище, Ім’я, По батькові, РНОКПП, Номер контактного телефону, Адреса електронної пошти
31	Прізвище, Ім’я, По батькові, РНОКПП, Дані ідентифікаційного документу
32	Прізвище, Ім’я, По батькові, РНОКПП, Дата народження, Громадянство, Стать

41	Прізвище, Ім’я, По батькові, РНОКПП, Дані ідентифікаційного документу, Номер контактного телефону, Адреса електронної пошти
42	Прізвище, Ім’я, По батькові, РНОКПП, Дата народження, Громадянство, Стать, Номер контактного телефону, Адреса електронної пошти
51	Прізвище, Ім’я, По батькові, РНОКПП, Дані щодо місця перебування або проживання, Дані ідентифікаційного документу, Дата народження, Громадянство, Стать
61	Прізвище, Ім’я, По батькові, РНОКПП, Дані щодо місця перебування або проживання, Дані ідентифікаційного документу, Дата народження, Громадянство, Стать, Номер контактного телефону, Адреса електронної пошти
71	Прізвище, Ім’я, По батькові, РНОКПП, Дані щодо місця перебування або проживання, Дані ідентифікаційного документу, Дата народження, Громадянство, Стать, Номер контактного телефону, Адреса електронної пошти, Соціальний статус, в т.ч. місце роботи та посада Інформація про публічно відому особу, застосування санкцій та ін.

Приклад відображення назви абонентського вузла Абонента-надавача послуг/Абонента-надавача послуг зі спеціальним статусом від якого було

ініційовано запит та тексту з інформацією по 11 номеру стандартизованого набору даних:

Дані будуть передані до
Абонентський вузол Установи України

Буде передано наступні дані:
Прізвище, Ім’я, По батькові,
Дані щодо місця перебування або проживання.

Додаток 3
до Специфікації взаємодії абонентського
вузла з центральним вузлом Системи BankID
Національного банку України

Ідентифікатори подій

Ідентифікатор події	Відправник та отримувач запиту	Опис події
GET1	Абонент-надавач послуг --> Центральний вузол	Запит Абонента-надавача послуг до Центрального вузла методом GET на отримання коду авторизації (authorization_code) (перший етап) п.2.1.1
GET4	Центральний вузол --> Абонент-ідентифікатор	Запит до абонентського вузла Абонента-ідентифікатора методом GET і отримання коду авторизації (authorization_code) (перший етап) п.2.2.1
GET6	Абонент-ідентифікатор--> Центральний вузол	Переадресація користувача у разі його успішної багатофакторної автентифікації Абонентом-ідентифікатором з абонентського вузла до Центрального вузла п.2.1.1
POST8	Центральний вузол --> Абонент-ідентифікатор	Запит Центрального вузла до абонентського вузла Абонента-ідентифікатора на отримання коду доступу (access_token) методом POST (другий етап) п.2.2.2
ResponsPOST8	Абонент-ідентифікатор--> Центральний вузол	Відповідь Абонента-ідентифікатора на POST8 п.2.2.2
GET10	Центральний вузол --> Абонент-надавач послуг	У разі успішної багатофакторної автентифікації користувача Абонентом-ідентифікатором, Центральний вузол виконує переадресацію запиту користувача до абонентського вузла Абонента-надавача послуг із кодом авторизації (authorization_code) на зареєстрований параметр callback_url п.2.1.1
POST11	Абонент-надавач послуг --> Центральний вузол	Запит Абонента-надавача послуг до Центрального вузла на отримання коду доступу (access_token) методом POST (другий етап) п.2.1.2

ResponsPOST11	Центральний вузол --> Абонент-надавач послуг	Відповідь центрального вузла на POST11 п.2.1.2
POST13	Абонент-надавач послуг --> Центральний вузол	Запит на дані від абонентського вузла Абонента-надавача послуг до Центрального вузла п.2.3.1
POST15	Центральний вузол --> Абонент-ідентифікатор	Запит на дані від Центрального вузла до абонентського вузла Абонента-ідентифікатора п.2.3.2
ResponsPOST15	Абонент-ідентифікатор--> Центральний вузол	Відповідь Абонента-ідентифікатора на POST15 п.2.3.2
ResponsPOST13	Центральний вузол --> Абонент-надавач послуг	Відповідь Центрального вузла на POST13 п.2.3.1

Додаток 4
до Специфікації взаємодії абонентського
вузла з центральним вузлом Системи BankID
Національного банку України

Електронний звіт журналу аудиту

Абонентського вузла Абонента-ідентифікатора (А-І)

Назва вузла А-НП, memberID	Назва вузла А-І, memberID	Ідентифікатор сесії sidBi	GET запит на ідентифікацію	POST запит на код доступу ЦВ до А-І	*А-І не заповнює*	*А-І не заповнює*	Запит на дані	Номер набору даних
1	2	3	4	5	6	7	8	9
		sidBi	Час	Час Код доступу			Час ЕПІ успішне/ неуспішне	

Абонентського вузла абонента-надавача послуг/Абонента–надавача послуг зі спеціальним статусом (А-НП)

Назва вузла А-НП, memberID	Назва вузла А-І, memberID	Ідентифікатор сесії state	GET запит на ідентифікацію	*А-НП не заповнює*	GET запит від ЦВ до АНП з кодом авторизації ЦВ	Запит на код доступу до ЦВ	Запит на дані	Номер набору даних
1	2	3	4	5	6	7	8	9
		state	Час		Час Код авторизації	Час Код доступу	Час ЕПІ успішне/ неуспішне	

Центрального вузла (ЦВ)

Назва вузла А-НП, memberID	Назва вузла А-І, memberID	Ідентифікатори сесії: • ЦВ sidBi • АНП state	GET запит на ідентифікацію	POST запит на код доступу ЦВ до А-І	GET запит від ЦВ до АНП з кодом авторизації ЦВ	Запит А-НП до ЦВ на код доступу	Запит на дані	Номер набору даних
1	2	3	4	5	6	7	8	9

		sidBi state	Час	Час Код доступу	Час Код авторизації	Час Код доступу	Час ЕПІ успішне/ неуспішне	