Національний банк України
Рада Системи BankID Національного банку України

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

Специфікація взаємодії абонентського вузла абонента-ідентифікатора з центральним вузлом Системи BankID Національного банку України

Київ 2021

Аркуш контролю версій

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

4.2	30.03.2021	Ключ ‘*issueCountryIso2’* вилучено із переліку ключів, обов’язкових для заповнення. Внесено уточнення щодо передачі даних по ключу ‘*documents’*.

ЗМІСТ

Глосарій

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

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

1. Загальна частина

1.1. Призначення документа

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

1.2. Цілі створення сервісу

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

1.3. Концепція функціонування системи

Функціонально система складається з трьох основних блоків:

1. ***ПП (*вебсайт (вебпортал), мобільний застосунок*)***, на якому розміщені форми надання послуг у електронному вигляді. Під час входу на портал або замовлення послуги користувачу доступна можливість авторизації або ідентифікації за допомогою Системи BankID НБУ у вигляді банера або кнопки.

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

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

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

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

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

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

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

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

3. ***Банк (АБС: вебпортал інтернет-банкінгу або іншого сервісу банку)***, на вебсторінці якого має бути реалізована форма ідентифікації користувача,

програмні процедури автоматичного формування коду авторизації (**authorization_code**), коду доступу (**access_token**) та електронної анкети (п. 2.2), накладення на неї кваліфікованої електронної печатки банку, шифрування даних анкети і переспрямування цієї анкети до ПП.

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

сформувати код авторизації (**authorization_code**), за яким здійснюється запит на отримання коду доступу (**access_token**);

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

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

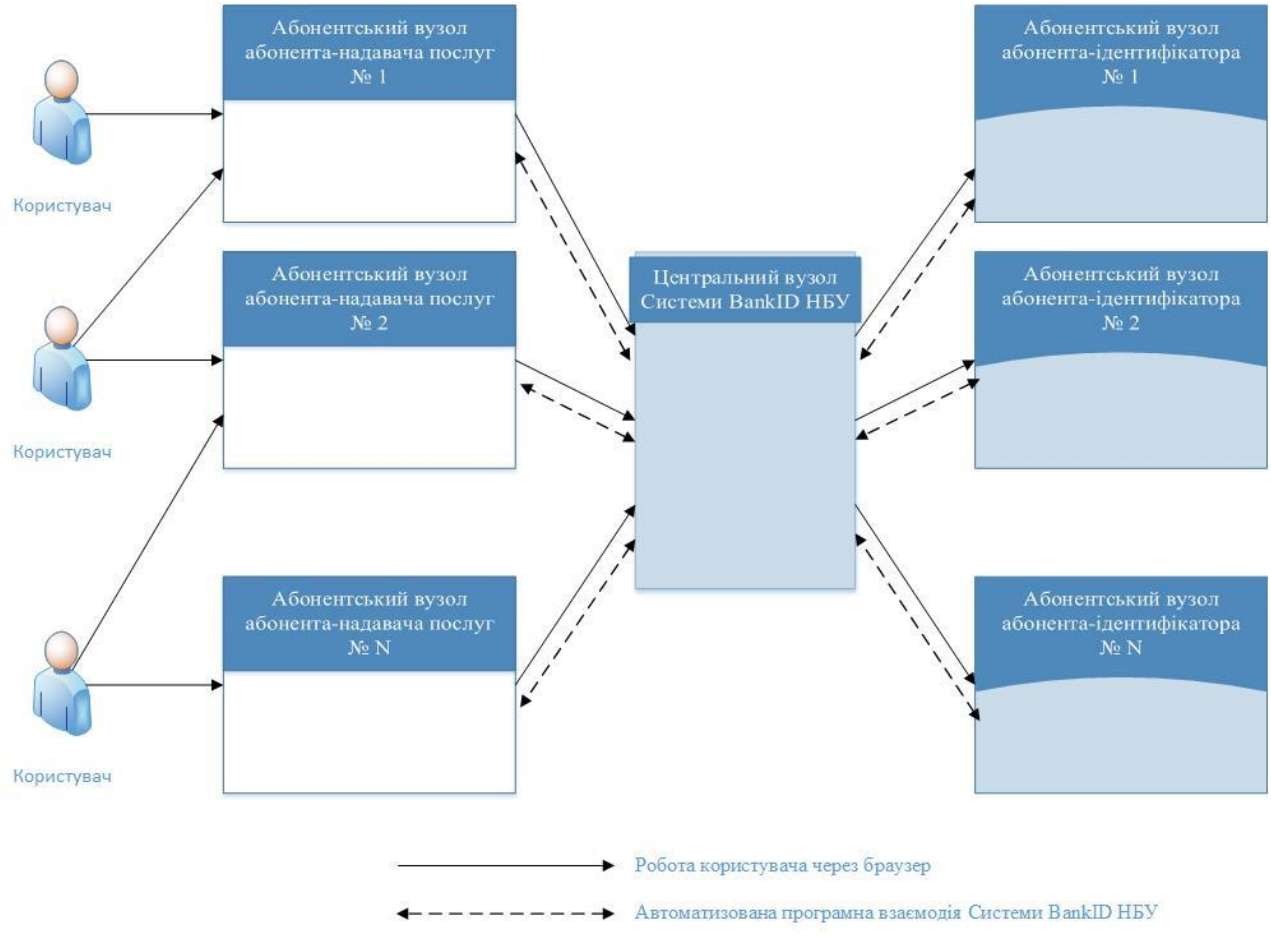

Рис. 1. Загальна схема функціонування Системи BankID НБУ

2. Технічна архітектура системи

Взаємодія центрального вузла Системи BankID НБУ з АБС відбувається на базі протоколу OAuth2.0 згідно зі специфікацією (що розташована за вебадресою http://tools.ietf.org/html/rfc6749). Рекомендовано використовувати готові рішення з вебсайта http://oauth.net/2/ – секція "*Code and Services"*, варіанти під усі популярні платформи та мови програмування.

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

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

Для підключення банку до ц. в. Системи BankID НБУ уповноважена особа від банку надає вебадресу АБС банку, на яку ініціюватимуться запити від ц. в. Системи BankID НБУ до АБС (**login_url**) та вебадреси, на які здійснюватимуться запити на код доступу (**token_api_url**) та на персональні дані (**data_api_url**) від ц. в. BankID НБУ. Адміністратор ц. в. Системи BankID НБУ видає уповноваженій особі банку унікальні ідентифікатори параметрів з'єднання (**client_id, client_secret**). Усі зазначені параметри обов'язкові, мають бути фіксовані і не повинні містити змінних параметрів (зміни в адресах повинні узгоджуватися з адміністратором центрального вузла Системи BankID НБУ).

Параметр	Опис
client_id	Унікальний ідентифікатор ресурсу АБС, виду стрічки 32-шістнадцяткових значень, розділеної на групи дефісами. Надається адміністратором ц. в. BankID НБУ під час реєстрації, наприклад: 95e4ba81-06ad-4e97-b9d9-0728fbed074f
client_secret	Унікальний ідентифікатор секрету ресурсу АБС, виду стрічки 32-шістнадцяткових значень. Надається адміністратором ц. в BankID НБУ під час реєстрації, наприклад: 5d42123a80942fda030c893c951fc08

login_url	Вебадреса АБС банку, на яку буде переадресовано користувача з вебсторінки ц. в. BankID НБУ. Надається стороною банку під час реєстрації, наприклад: https://bank.example.com.ua/oauth2/authorize Вебадреса буде доповнена параметрами та значеннями згідно з п. 2.1.1
token_api_url	Вебадреса АБС банку, на яку здійснюватиметься запит для отримання коду доступу (**access_token**). Надається банком під час реєстрації, наприклад: https://bank.example.com.ua/oauth2/v1/bankid/token
data_api_url	Вебадреса АБС банку, на яку здійснюватиметься запит для отримання персональних даних користувача. Надається банком під час реєстрації, наприклад: https://bank.example.com.ua/oauth2/v1/bankid/client

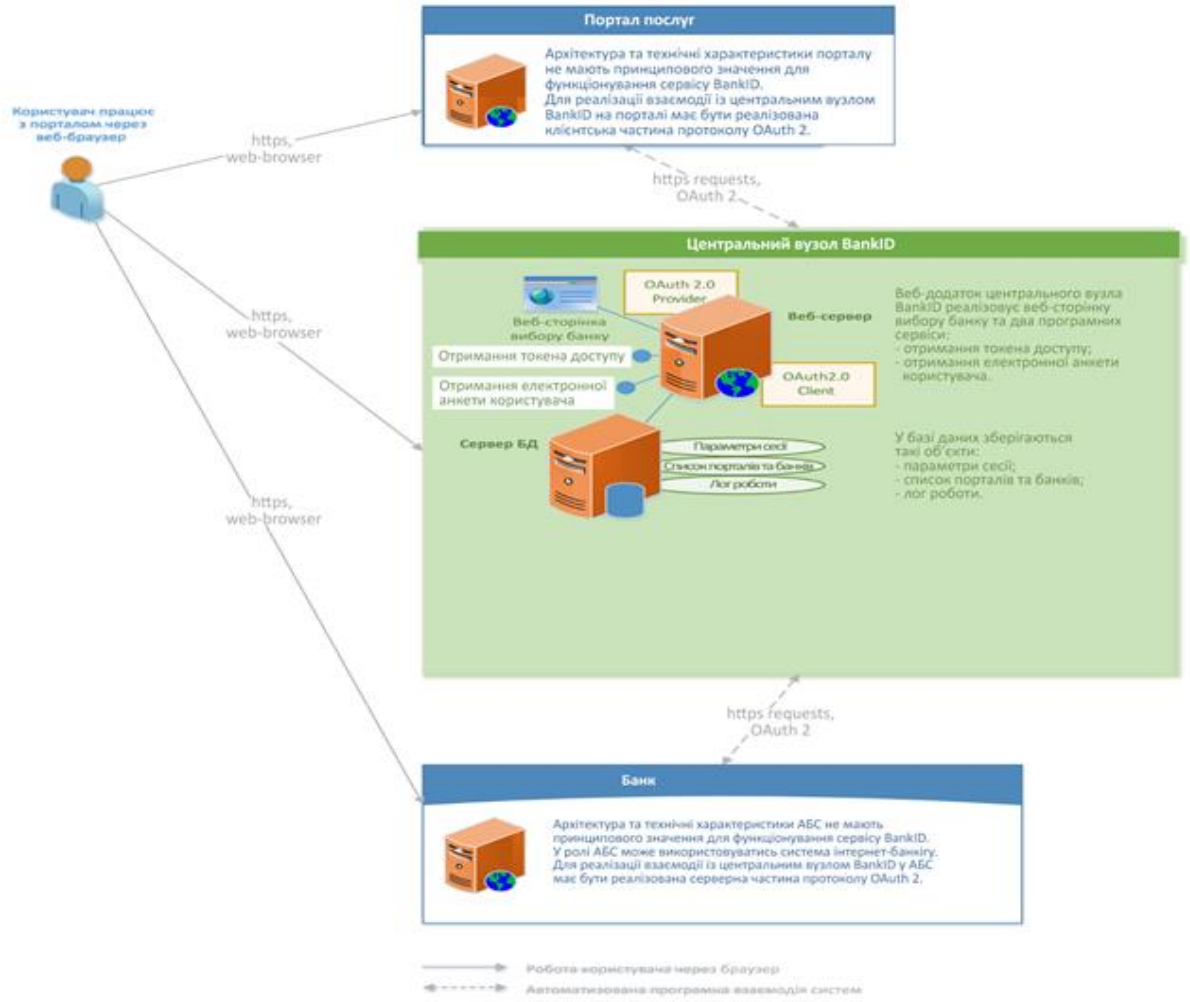

Рис. 2. Технологічна схема функціонування Системи BankID НБУ

2.1. Процедура авторизації

Авторизація згідно зі стандартом OAuth 2.0 виконується у два етапи:

перший етап – отримання коду авторизації (**authorization_code)**, параметр отриманий у запиті на вебадресу **callback_url**, вказану в запиті п. 2.1.1;

другий етап – отримання коду доступу (**access_token**) на підставі коду авторизації (запит на адресу банку, значення параметра **token_api_url**, вказану під час реєстрації, п. 2.1.2).

Примітка. Вебсторінка АБС банку, на якій користувач проходить процедуру автентифікації та погоджує процес передачі персональних даних, повинна містити назву банку-ідентифікатора та ТМ, мати контактний телефон гарячої лінії з можливістю переходу користувача на вебсторінку з контактною інформацією відповідного банку або форму зворотного зв'язку.

2.1.1. Перехід на сторінку АБС методом GET (перший етап)

Структура запиту від ц. в. BankID НБУ до АБС, запит формується під час переадресації користувача з банера банку на вебсторінці ц. в. BankID НБУ у такому форматі:

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

Параметр	Опис
callback_url	Вебадреса ц. в. BankID НБУ, на яку буде виконано запит із кодом авторизації (**authorization_code**) і на яку буде виконано переадресацію користувача. Адреса фіксована, не повинна містити змінних параметрів
state	Ідентифікатор сесії. Генерується з боку ц. в. BankID НБУ і має бути повернутий в запиті з кодом авторизації на вебадресу ц. в. BankID НБУ, вказану у значенні **callback_url** або у випадку помилок. Наприклад: 2baeadd0-c7e6-4ad9-9181-1fd9bbebfaac

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

```
GET https://bank.example.com.ua/v1/bank/oauth2/authorize?
   response_type=code&
   client_id=95e4ba81-06ad-4e97-b9d9-0728fbed074f&
   redirect_uri=https://id.bank.gov.ua/v1/bank/oauth2/callback/code&
   state=2baeadd0-c7e6-4ad9-9181-1fd9bbebfaac
```

Відповідь АБС банку:

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

У разі успішної автентифікації користувача на стороні АБС банку система банку повинна зробити запит із кодом авторизації **authorization_code** на адресу параметра **redirect_uri.** Із даним запитом відбувається переадресація користувача до ц. в. BankID НБУ.

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

```
GET https://id.bank.gov.ua/v1/bank/oauth2/callback/code?
   code=authorization_code&
   state=state
HTTP/1.1
```

Параметр	Опис
authorization_code	Код авторизації — певний унікальний ідентифікатор який формується на стороні АБС банку.
state	Буде вказано значення ідентифікатора сесії який передав ц.в. BankID НБУ.

Приклад запиту від АБС банку:

```
GET https://id.bank.gov.ua/v1/bank/oauth2/callback/code?
   code=2d6f2318cb06cc2c97d948deb9799d608f1d5c97&
   state=2364fc5d-c6b6-4f99-87a9-11d2baa32484
```

Можливі помилки.

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

• некоректний запит центрального вузла (зокрема, ц. в. BankID НБУ не зареєстрований на стороні банку або не збігається значення певного параметра в запиті). У такому випадку опис помилки повинен бути відображений на вебсторінці АБС.

• користувача не вдалося автентифікувати на стороні АБС банку – буде виконано запит із переадресацією користувача на адресу значення **redirect_uri** з можливими значеннями помилок у параметрах запиту, наприклад:

```
GET https://id.bank.gov.ua/v1/bank/oauth2/callback/code?
   error=access_denied&
   error_description=No_rights_for_BankID&
   state=2364fc5d-c6b6-4f99-87a9-11d2baa32484
HTTP/1.1
```

Параметр	Опис
error	Один із визначених кодів помилки згідно зі специфікацією OAuth2.0 (https://tools.ietf.org/html/rfc6749#section-4.1.2.1). Зокрема: ***invalid_request*** – у запиті відсутні обов'язкові значення або недопустимі значення певного параметра; ***unauthorized_client*** – неможливо отримати код авторизації; ***access_denied*** – запит заборонений.
error_description	Можливий текстовий опис помилки, деталізація для розробників
state	Буде вказано значення ідентифікатора сесії який передав ц.в. BankID НБУ.

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

Після отримання запиту з кодом авторизації ц. в. BankID ініціює запит на отримання коду доступу. Структура запиту від ц. в. BankID НБУ до АБС, за якого значення передаються у вигляді стрічки з параметрами на вебадресу, що надана банком під час реєстрації **token_api_url** п. 2 у такому форматі:

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

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

У відповідь АБС банку надає параметри та значення коду доступу в тілі запиту (*body*) у Json-форматі. Опціонально: у відповіді параметр зі значенням **refresh_token** зазначається, якщо термін дії коду доступу (**access_token**) досить короткий і на ресурсі АБС банку реалізований даний функціонал для оновлення запиту.

Приклад відповіді ц. в. BankID:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
   "token_type":"bearer",
   "access_token":"db8814c6d97cbad2a02db80e17d4676fab5914c6",
   "expires_in":3600,
   "refresh_token":"91ee282ccda4e1af6dbd0da4920b206866278f5e"
}
```

Параметр	Опис
token_type	Указується тип запиту під час якого передається код доступу, який повинен мати значення **“bearer”**

access_token	Значення коду доступу
expires_in	Термін дії коду доступу (значення в секундах)
refresh_token	Код оновлення запиту (опціонально, якщо підтримується АБС)

Можливі помилки.

У разі виникнення помилок оброблення запиту рекомендуємо орієнтуватися на список кодів стану HTTP. У відповідь АБС надає параметри зі значеннями помилки, що спричинили відмову, і передає у тілі відповіді (*body*) у Json-форматі.

Приклад тіла 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). Наприклад: **invalid_request** - у запиті немає обов'язкових значень або неправильно сформованих значень одного або декількох параметрів; **invalid_grant** - некоректний код авторизації (authorization_code) або термін дії коду авторизації вичерпано.
error_description	Можливий текстовий опис помилки, деталізація для розробників
code	Буде вказано значення коду авторизації при якому виникла помилка (authorization_code)

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

Якщо зі сторони АБС банку отримана відповідь зі значенням параметра **refresh_token**, то для можливості продовжити дію вже отриманого коду доступу (без необхідності виконання всіх попередніх викликів) необхідно виконати такий запит.

Структура запиту від ц. в. BankID НБУ до АБС, значення передаються у вигляді стрічки з параметрами на вказану вебадресу банку (надавалася банком під час реєстрації **token_api_url**, п. 2) у такому форматі:

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

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

У відповідь АБС банку надає параметри та значення коду доступу в тілі запиту (*body*) в Json-форматі.

Приклад відповіді АБС банку:

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

2.2. Процедура отримання даних користувача

Надання даних відбувається на підставі коду доступу (**access_token**), отриманого в ході авторизації (згідно з попереднім пунктом). Код доступу передається в заголовку запиту (**headers**) у вигляді:

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

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

набір даних від ПП до АБС, у якому було здійснено автентифікацію користувача як клієнта банку.

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

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

Приклад Json-об’єкта на запит персональних даних:

```
{
   "memberId":"1111111101",
   "sidBi":"2baeadd0-c7e6-4ad9-9181-1fd9bbebfaac",
   "cert":"inThisValuePortalProvideYourCertificateEncodeToBase64Format==",
   "type":"physical",
   "fields":[
      "firstName","middleName","lastName","phone","inn","birthDay","sex",
      "flagPEPs","flagPersonTerror","flagRestriction","flagTopLevelRisk"
   ],
   "addresses":[
      {"type":"factual","fields":[
         "country","state","area","city","street","houseNo","flatNo"
      ]},
      "type":"juridical","fields":[
         "country","state","area","city","street","houseNo","flatNo"
      ]}
   ],
   "documents":[
      {"type":"passport","fields":[
         "series","number","issue","dateIssue","dateExpiration","issueCountryIso2"
      ]},
      {"type":"zpassport","fields":[
         "series","number","issue","dateIssue","dateExpiration","issueCountryIso2"
      ]}
   ],
   "scans":[
      {"type":"passport","fields":["scanFile","dateCreate","extension"]},
      {"type":"zpassport","fields":["scanFile","dateCreate","extension"]}
   ]
}
```

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

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

Ключ			Значення ** (формат та вимоги)	Опис
1	2	3	4	5
cert*			Закодовано по стандарту BASE64.	Кваліфікований сертифікат шифрування
memberId			XXXXXXXXNN – де: XXXXXXXX – ідентифікатор абонента (код ЄДРПОУ); NN – порядковий номер абонентського вузла. Ключ та значення "memberId" додаються ц. в. BankID НБУ.	Унікальний ідентифікатор вузла абонента в Системі BankID НБУ
sidBi			Ключ та значення додаються ц. в. BankID НБУ.	Ідентифікатор сесії
type			physical	Значення ідентифікації фізичної особи. На даний час приймає тільки одне значення – physical.
	fields	**Масив з даними по особі**		
		lastName*		Прізвище
		firstName*		Ім’я
		middleName*		По батькові
		phone	380XXXXXXXXX - де X може приймати тільки цифрове значення.	Номер телефону
		inn*	Заповнюється відповідно до вимог законодавства України	Реєстраційний номер облікової картки платника податків, номер (та за наявності - серію) паспорта громадянина України, в якому проставлено відмітку про відмову від прийняття реєстраційного номера облікової картки платника податків, чи номер паспорта із записом про відмову від прийняття реєстраційного номера облікової картки платника податків в електронному безконтактному носії.
		clId		Унікальний ідентифікатор клієнта в банку. У випадку якщо банк не має такого ідентифікатора, можливо вказати значення ключа inn або серію й номер паспорта.
		clIdText	“Інформація надана засобами Системи BankID НБУ dd.mm.yyyy hh.mm”	Статичний текст з інформацією про надані дані банком щодо користувача, дата і час надання
		birthDay*	dd.mm.yyyy	Дата народження.
		sex*	Можливі значення:	Стать

Ключ			Значення ** (формат та вимоги)	Опис
1	2	3	4	5
			латинська літера M – чоловіча або F – жіноча	
		email		Електронна адреса
		socStatus	Наприклад: “студент”, “пенсіонер”, “тимчасово безробітний”, “працюючий”, “нерегулярна зайнятість”.	Соціальний статус
		flagPEPs	Можливі значення: 1 – так, 0 – ні.	Ознака, чи визначена фізична особа банком-повіреним такою, що належить до категорії PEPs (публічні особи, близькі, пов’язані).
		flagPersonTerror	Можливі значення: 1 – так, 0 – ні.	Ознака, чи визначена фізична особа банком-повіреним такою, що включена до переліку осіб, пов’язаних зі здійсненням терористичної діяльності або щодо яких застосовано міжнародні санкції.
		flagRestriction	Можливі значення: 1 – так, 0 – ні.	Ознака, чи визначена фізична особа банком-повіреним такою, що включена до переліку осіб, щодо яких застосовані персональні, спеціальні економічні та інші обмежувальні заходи (санкції), санкції РНБОУ.
		flagTopLevelRisk	Можливі значення: 1 – так, 0 – ні.	Ознака, чи присвоєний клієнту банком-повіреним (неприйнятно) високий рівень ризику ПВК/ФТ.
		uaResident	Можливі значення: 1 – так, 0 – ні.	Ознака, чи визначена фізична особа банком-повіреним такою, що є резидентом України.
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*	Двозначний літерний код країни за стандартом ISO_3166-1 (alfa-2). Наприклад: UA	Країна
		state*		Область. Якщо адреса користувача не передбачає наявності області, відповідне значення не передається у відповіді абонента-ідентифікатора.
		area*		Район. Якщо адреса користувача не передбачає наявності району, відповідне значення не передається у відповіді абонента-ідентифікатора.
		city*		Місто
		street*		Вулиця

Ключ			Значення ** (формат та вимоги)	Опис
1	2	3	4	5
		houseNo*		Номер будинку
		flatNo*		Номер квартири. Якщо адреса користувача не передбачає наявності номеру квартири, відповідне значення не передається у відповіді абонента-ідентифікатора.
documents	**Масив типів документів та реквізити документів що засвідчують особу**			
	type*		Можливі значення: **passport,** **idpassport,** **zpassport,** **ident.**	Тип документу: **passport** – паспорт; **idpassport** – id-картка; **zpassport** – закордонний паспорт; **ident** – посвідчення особи у відповідності до вимог законодавства України.
	fields	**Масив реквізитів документів що засвідчують особу**		
		typeName*		Назва документу
		series*		Серія документа (для типу **idpassport** - не заповнюється).
		number*		Номер документа
		issue*		Яким органом видано документ
		dateIssue*	dd.mm.yyyy	Дата видачі документу
		dateExpiration*	dd.mm.yyyy	Термін дії (для типу **passport** - не заповнюється)
		issueCountryIso2	Двозначний літерний код країни за стандартом ISO_3166-1 (alfa-2). Наприклад: UA	Країна видачі документа
scans	**Масив скан-копій з типами та файлами документів особи**			
	type		Можливі значення: **passport,** **idpassport,** **zpassport,** **inn,** **personalPhoto.**	Тип відсканованого документа: **passport** – паспорт; **idpassport** – id-картка; **zpassport** – закордонний паспорт; **inn** – реєстраційний номер облікової картки платника податків; **personalPhoto** – фото особи (анфас).
	fields	**Масив з файлів скан-копій**		
		scanFile	Закодований по стандарту BASE64. Якщо скан-копія знаходиться в архіві, то файл скан-копій обов'язково повинен мати розширення (наприклад: pdf, jpg, png, bmp).	Файл сканованої копії документу. Рекомендована роздільна здатність скан-копії не менше 200 DPI.
		dateCreate	dd.mm.yyyy	Дата створення скан-копії документа
		extension	У випадку, якщо файли об'єднанні або заархівовані у zip форматі, то зазначається	Розширення файлу, який знаходиться в значенні ключа scanFile.

Ключ			Значення ** (формат та вимоги)	Опис
1	2	3	4	5
			розширення zip.	

* - обов’язкові ключі для заповнення абонентом-ідентифікатором.
** - всі значення ключів мають символьний тип.

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

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

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

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

У разі запиту абонента-надавача послуг на отримання даних клієнта:
за документом паспорт громадянина України (“passport”) ключ “dateExpiration” не є обов’язковим до заповнення;

за документом id-картка (“idpassport”) ключ “series” не є обов’язковим до заповнення.

Значення ключа “scans” заповнюється абонентом-ідентифікатором виключно на запит банків, зареєстрованих у Системі BankID НБУ у статусі абонентів-надавачів послуг та може бути використана такими абонентами – надавачами послуг виключно для надання фінансових послуг без права передавання її третім особам.

2.2.2. Запит даних користувача, як клієнта банку

Для отримання даних щодо користувача направляється запит від ц. в. BankID НБУ до АБС за вебадресою, наданою банком під час реєстрації (**data_api_url**) п. 2. Параметри та значення передаються в тілі запиту (*body*) в Json-форматі.

Приклад запиту щодо даних до АБС банку:

```
POST https://bank.example.com.ua/v1/bank/resource/client  HTTP/1.1
Authorization: Bearer access_token
Content-Type: application/json
{
   "memberId":"1111111101",
   "sidBi": "2baeadd0-c7e6-4ad9-9181-1fd9bbebfaac",
   "cert":"dEBIGx1pdL6dt1ngaOEfPvt/ik9eUpDuz90rm/Vk23v+FtiKJEvGnu
ea9FGjvBMGlFZS4zhg2IYIHGOhlBVYrZcez6udotjZlCLGZ7zwPuFo0XypKD
Qj5qpR7w0rFFZNjcPH3JW2IzEUv…….",
   "type":"physical",
   "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","dateExpiration","issueCountryIso2"
      ]}
   ],
   "scans":[
      {"type":"passport","fields":[
         "scanFile","dateCreate","extension"
      ]}
   ]
}
```

Параметр	Опис
access_token	Код доступу, отриманий у відповіді від АБС

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

Приклад відповіді:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
   "state": "ok",
   "cert":"dEBIGx1pdL6dt1ngaOEfPvt/ik9eUpDuz90rm/Vk23v+FtiKJEvGnu
ea9FGjvBMGlFZS4zhg2IYIHGOhlBVYrZcez6udotjZlCLGZ7zwPuFo0XypKDQj5
qpR7w0rFFZNjcPH3JW2IzEUv…….",
   "customerCrypto":
“dEBIGx1pdL6dt1ngaOEfPvt/ik9eUpDuz90rm/Vk23v+FtiKJEvGnuea9FGjvBMGl
FZS4zhg2IYIHGOhlBVYrZcez6udotjZlCLGZ7zwPuFo0XypKDQj5qpR7w0rFFZ
NjcPH3JW2IzEUv/4bXQWqYCccma03b3lbva+YJ/Txox1CMfyV4jJ5fXeCMOjE
WxwctEc7mXNzPfcbKMoqr048uvW9HTiPkjsLIU5jgTKJVdgoanZI4712dmQev5
UzMKqNYvOwfJ+hU872kCSD1wfgVaJU0qP6yURcK80ys2K5OvUpa9uIHwmL7
KmnxMDhB4hLr5CQPl1XZ09RnNykgS/4cQ…….”
 }
```

Шифрування підписаних персональних даних відбувається відповідно до вимог до форматів криптографічних повідомлень, визначених наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 18.12.2012 № 739 (http://zakon3.rada.gov.ua/laws/show/z0108-13) (далі – Вимоги). Узгодження ключів за замовчуванням здійснюється з використанням статичного механізму. Якщо параметри криптографічного алгоритму статичної ключової пари відправника не еквівалентні параметрам криптографічного алгоритму статичної ключової пари одержувача, повинен здійснюватися перехід до застосування динамічного механізму узгодження ключів. Засоби криптографічного захисту інформації відправника та одержувача повинні підтримувати криптографічні алгоритми, визначені цими Вимогами.

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

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

```
   "email":"geraschenko@gmail.com",
   "birthDay":"20.01.1953",
   "firstName":"ПЕТРО",
   "lastName":"ГЕРАЩЕНКО",
   "middleName":"ІВАНОВИЧ",
   "phone":"380961234511",
   "clId":"6299E05EC5D568733C14CCEF9C975DD3",
   "clIdText":"Інформація надана засобами Системи BankID НБУ 25.12.2017
19:40",
   "socStatus": "пенсіонер",
   "flagPEPs":"0",
   "flagPersonTerror":"1",
   "flagRestriction":"0",
   "flagTopLevelRisk":"1",
   "uaResident":"1",
   "addresses": [{
      "type":"factual",
      "country":"UA",
      "state":"ВОЛИНСЬКА",
      "city":"Ківерці",
      "street":"Незалежності",
      "houseNo":"62",
      "flatNo":"12"
   }],
   "documents":[{
      "type":"passport",
      "series":"AA",
      "number":"222333",
      "issue":"Ківерцівським РО УМВД",
      "dateIssue":"15.03.1999",
      "issueCountryIso2":"UA"
   }],
   "scans":[{
      "type":"passport",
      "scanFile":"H4sIAAAAAAAAEAOS8dVhczZYuHtxdQiBA4wRraNwdg
ru7NO7uFpwEd3cLwTEd3cLwEd3cLwEd3cLwEd3cLwEd3cLwE.....",
      "dateCreate":"09.04.2015",
      "extension":"zip"
   }]
}
```


Після цього вказаний Json-об’єкт підписується кваліфікованою електронною печаткою банку і шифрується симетричним ключем сеансу

(КШД – ключ шифрування даних за алгоритмом, визначеним у ДСТУ ГОСТ 28147-2009). Підписаний та зашифрований об’єкт формується у вигляді цифрового конверта згідно з Вимогами.

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

Можливі помилки.

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

Приклад технічної помилки:

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

Приклад логічної помилки:

{"**error**":"invalid_cert", "**error_description**":"Sertificate not found at EUSignCP.EUPackHelper.EnvelopData(Byte[] data)", "**code**":"CL003"}

Параметр	Опис
error	Приклади технічних помилок: **invalid_request** – у запиті немає обов’язкових або неправильно сформованих значень; **invalid_token** – некоректний код доступу (**access_token**) або термін дії коду доступу вичерпано. Приклад логічних помилок: **invalid_cert** – проблеми під час оброблення кваліфікованого сертифікату, зокрема некоректний/недійсний сертифікат або проблеми з підписом; **invalid_data** – ключі в запиті щодо користувача некоректні.
error_description	Текстовий опис помилки, деталізація для розробників
code	Певне значення, яке може допомогти банку для аналізу причини помилки.

3. Захист інформації в Системі BankID НБУ

3.1. Загальні положення

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

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

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

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

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

Журнал аудиту центрального вузла Системи BankID НБУ повинен містити відомості про факт проходження електронного запиту на ідентифікацію від абонента – надавача послуг через центральний вузол Системи BankID НБУ абоненту-ідентифікатору, про факт проходження електронного підтвердження ідентифікації від абонента-ідентифікатора через центральний вузол Системи BankID НБУ абоненту – надавачу послуг.

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

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

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

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

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

Наприклад:

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

- ідентифікацію буде дозволено, якщо запит з параметрами
  redirect_uri = https://example.com.ua
  redirect_uri = https://example1.example.com.ua
- ідентифікацію не буде дозволено, якщо запит з параметром
  redirect_uri = https://exammmmple.com.ua

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

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

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

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

Абонентські вузли та ц. в. Системи BankID НБУ для встановлення безпечного з’єднання між собою та з користувачами Системи BankID НБУ повинні використовувати криптографічний протокол TLS не нижче версії 1.2, а також відповідні особисті ключі та сертифікати відкритих ключів.

У протоколі TLS допускаються різні криптографічні набори.

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

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

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

Не рекомендується застосовувати криптографічні набори, які для обміну ключами 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.

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

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

− накладає на електронне підтвердження ідентифікації кваліфіковану електронну печатку;

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

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

Шифрування/розшифрування електронного підтвердження ідентифікації відбувається згідно з алгоритмами та правилами, визначеними Вимогами до форматів криптографічних повідомлень, які затверджені наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 (http://zakon3.rada.gov.ua/laws/show/z0108-13). Узгодження ключів шифрування за умовчанням 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.

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