ДЕРЖАВНЕ АГЕНТСТВО
з питань електронного урядування України

Інтегрована система електронної ідентифікації

Порядок обробки інформації у системі

ЄААД.468244.209 Д7.01

2019 р.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

БД	-	База даних
ЕОТ	-	Електронна обчислювальна техніка
ЕЦП	-	Електронний цифровий підпис
ІТС	-	Інформаційно-телекомунікаційна система
КЗЗ	-	Комплекс засобів захисту
КСЗІ	-	Комплексна система захисту інформації
КТЗ	-	Комплекс технічних засобів
ЛОМ	-	Локальна обчислювальна мережа
МЕ	-	Міжмережний екран
МКМ	-	Мережний криптомодуль
НКІ	-	Носій ключової інформації
НСД	-	Несанкціонований доступ
ПЗ	-	Програмний засіб
РС	-	Робоча станція
ТЗ	-	Технічне завдання
ЦЗО	-	Центральний засвідчуваний орган
ЦСК	-	Центр сертифікації ключів
CMP	-	Certificate management protocol (протокол управління сертифікатами)
HTTP	-	HyperText Transfer Protocol (протокол передачі гіпертекст)
HTTPS	-	HyperText Transfer Protocol Secure (безпечний протокол передачі даних)
IPS	-	Intrusion prevention system (система попередження вторжень)
OCSP	-	Online Certificate Status Protocol (протокол визначення статусу сертифіката)
PKCS	-	Public Key Cryptography Standarts (стандарти криптографії з відкритим ключем)
RDP	-	Remote Desktop (віддалений робочий стіл)
SQL	-	Structured Query Language (мова структурованих запитів)
SSH	-	Secure Shell (безпечна оболонка)
TCP	-	Transmission Control Protocol (протокол керування передачею)
TSP	-	TimeStamp Protocol (протокол формування мітки часу)
VPN	-	Virtual Private Network (віртуальна приватна мережа)

1 ЗАГАЛЬНИЙ ОПИС

Інтегрована система електронної ідентифікації (далі - Система) призначена для технологічного забезпечення зручної, доступної та безпечної електронної ідентифікації та автентифікації фізичних і юридичних осіб, підтримки її функціонування, сумісності та інтеграції схем електронної ідентифікації, їх взаємодії з web-порталами електронних послуг та системами електронної взаємодії органів влади, фізичних та юридичних осіб, забезпечення захисту інформації та персональних даних на основі єдиних вимог, форматів, протоколів та класифікаторів.

Об'єктами взаємодії системи визначаються:

- інформаційно-телекомунікаційні системи надання адміністративних та інших видів послуг в електронній формі;
- інформаційно-телекомунікаційні системи постачальників послуг електронної ідентифікації, які реалізують схеми електронної ідентифікації (ЦСК, власники інформаційно-телекомунікаційних систем банківських установ, оператори мобільного зв'язку тощо);
- інформаційно-телекомунікаційні системи, які реалізують схеми електронної ідентифікації в рамках транскордонної взаємодії.

Учасниками регламентних процедур та процесів, що підлягають автоматизації (далі - суб'єкти взаємодії) є:

- фізичні особи та фізичні особи-представники юридичних осіб, які звертаються до інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі - користувачі Системи;
- інформаційно-телекомунікаційні системи надання адміністративних та інших видів послуг в електронній формі;
- інформаційно-телекомунікаційні системи, які реалізують схеми електронної ідентифікації (акредитовані центри сертифікації ключів, власники інформаційно-телекомунікаційних систем банківських установ, оператори мобільного зв'язку тощо) - постачальники послуг електронної ідентифікації;
- інформаційно-телекомунікаційні системи, які реалізують схеми електронної ідентифікації в рамках транскордонної взаємодії.
- адміністратор (розпорядник) Системи;
- адміністратори проміжних вузлів (хабів) електронної ідентифікації.

Система забезпечує реалізацію таких компонентів цільового призначення:

- реалізація регламентних процедур та процесів електронної ідентифікації, фізичних та юридичних осіб для отримання ними адміністративних та інших видів послуг в електронній формі;
- забезпечення взаємодії та сумісності із інформаційно-телекомунікаційними системами, які реалізують схеми електронної ідентифікації та інформаційно-телекомунікаційними системами надання адміністративних та інших видів послуг в електронній формі;
- організаційне та технологічне забезпечення виконання вимог законодавства щодо захисту інформації та захисту персональних даних;
- розвиток Системи у напрямку інтеграції з інформаційно-телекомунікаційними системами в рамках транскордонної взаємодії;
- інтеграція інформаційно-телекомунікаційних систем суб'єктів інфраструктури електронної ідентифікації.

Система складається з сукупності таких функціонально пов'язаних підсистем:

- підсистема взаємодії зі схемами електронної ідентифікації ЦСК;
- підсистема взаємодії зі схемами електронної ідентифікації з використанням електронного посвідчення особи громадянина України (паспорта громадянина України у формі ID-картки);
- підсистема взаємодії з проміжними вузлами схем електронної ідентифікації банківських установ (BankID);
- підсистема взаємодії з проміжними вузлами схем електронної ідентифікації операторів мобільного зв'язку (MobileID);
- підсистема управління;
- підсистема захисту інформації.

2 ПОРЯДОК ОБРОБКИ ІНФОРМАЦІЇ

2.1 Загальна характеристика

Система під час функціонування взаємодіє з серверами прикладних систем, користувачами(клієнтами) прикладних систем, центрами сертифікації ключів, серверами мобільного підпису (оператора зв'язку), сервером банківської ідентифікації.

Порядок взаємодії складових частин Системи під час ідентифікації користувача (клієнта) на сервері прикладної системи реалізується відповідно до протоколу OAuth 2.0.

Для ідентифікації серверів прикладних систем на сервері ідентифікації, відповідні прикладні системи попередньо реєструються на сервері ідентифікації та згідно протоколу OAuth для кожної прикладної системи встановлюються наступні параметри:

- ідентифікатор прикладної системи **client_id**, який однозначно ідентифікує прикладну систему (значення ідентифікатора наведене для тестової прикладної системи зареєстрованої на тестовому сервері ідентифікації);
- секретна строчка доступу **client_secret**, за якою сервер ідентифікації буде видавати серверу прикладної системи маркер доступу - **access_token**;
- сертифікат відкритого ключа протоколу розподілу ключів прикладної системи, який призначений для направленого шифрування отриманої інформації про користувача (клієнта) при передачі між сервером ідентифікації та сервером прикладної системи.

2.2 Порядок електронної ідентифікації за електронним цифровим підписом

Структурно-функціональна схема електронної ідентифікації через центр сертифікації ключів (ЦСК, за електронним цифровим підписом – ЕЦП) та ідентифікації з використанням паспорта громадянина України у формі ID-картки наведена на рис. 2.1.

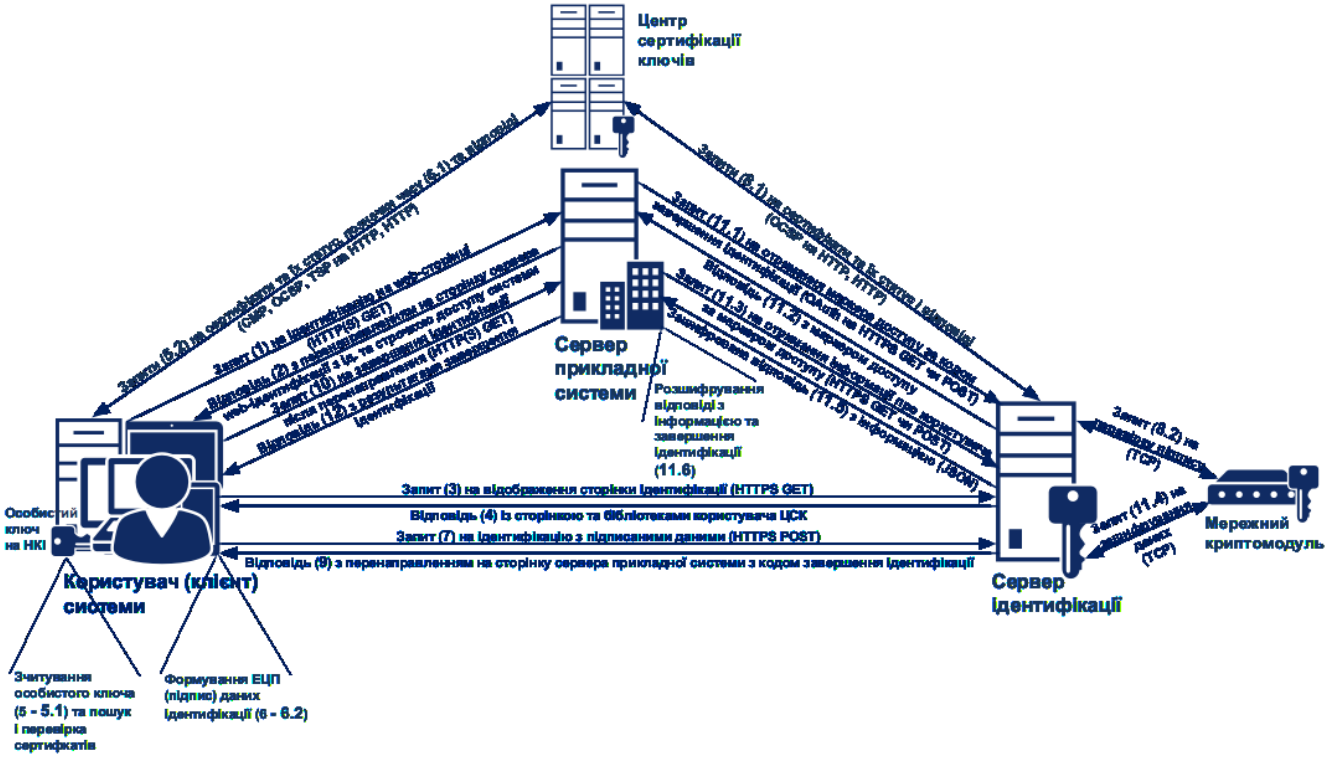

Рисунок 2.1 – Структурно-функціональна схема електронної ідентифікації через ЦСК та з використанням паспорта громадянина України у формі ID-картки

Порядок взаємодії складових частин Системи під час ідентифікації користувача (клієнта) Системи на сервері прикладної системи через ЦСК (за ЕЦП) та з використанням паспорта громадянина України у формі ID-картки повинен включати:

1)відправку користувачем (клієнтом) запиту на ідентифікацію з web-браузера на web-сторінці web-сервера прикладної системи (натискання посилання або контекстна відправка запиту) за методом GET протоколу HTTP(S);

2) обробку запиту та відправку web-сервером прикладної системи користувачеві відповіді із перенаправленням браузера користувача на відповідну сторінку сервера ідентифікації (перенаправлене посилання);

3) відправку користувачем запиту на відображення відповідної сторінки серверу ідентифікації за методом GET протоколу HTTPS на перенаправлене посилання виду:

```
GET
https://id.gov.ua/?response_type=code&
    client_id=client_id&
    auth_type=dig_sign,bank_id,mobile_id&
    state=state&
    redirect_uri= http(s)://url/redirect
```

Параметри запиту описані у табл. 2.2.1.

Таблиця 2.2.1 – Опис параметрів запиту користувача серверу ідентифікації

Параметри	Опис
response_type	Повинен мати значення **code**
client_id	Ідентифікатор прикладної системи (значення наведене для прикладу)
auth_type	Параметр, що визначає можливі засоби ідентифікації (задається перелік необхідних засобів аутентифікації, значення наведене для прикладу)
state	Параметр, значення якого має бути повернуто при переадресації на адресу, вказану у значенні **redirect_uri** (значення наведене для прикладу)
redirect_uri	Зворотне посилання (URI) на web-сервер прикладної системи (значення посилання **http(s)://url/redirect** наведене для прикладу), на яке сервер ідентифікації перенаправить браузер користувача після виконання процедури ідентифікації

Зворотне посилання (**redirect_uri**) також може бути попередньо встановлене не сервері ідентифікації разом із ідентифікатором прикладної системи (**client_id)** та секретною строчкою доступу (**client_secret)** у реєстраційних даних відповідної прикладної системи. У цьому випадку сервер прикладної системи може не передавати зворотне посилання у запиті, а сервер ідентифікації буде брати його з реєстраційних даних прикладної системи;

4) обробку запиту та відправку сервером ідентифікації користувачеві відповіді із вмістом web-сторінки ідентифікації та бібліотеками підпису користувача ЦСК (завантаження java-скрипта браузером чи підключення попередньо встановлених web-бібліотек підпису користувача ЦСК);

5) зчитування користувачем власного особистого ключа з використанням відповідної бібліотеки підпису, що включає:

5.1) зчитування файлу з особистим ключем java-скрипт-бібліотекою чи зчитування ключа з електронного ключа чи іншого носія ключової інформації або криптомодуля web-бібліотеками підпису з використанням пароля захисту;

5.2) відправку бібліотекою запиту у ЦСК на отримання ланцюжку сертифікатів користувача за протоколом CMP та отримання відповіді з ЦСК або зчитування сертифіката користувача з наданого файлу чи з постійного файлового сховища, відправку запитів на перевірку статусу сертифікатів у ЦСК за протоколом OCSP і отримання відповідей та завантаження з ЦСК поточних списків відкликаних сертифікатів (СВС) і перевірку статусу сертифікатів з використанням завантажених СВС;

6) формування користувачем ЕЦП - підпис даних ідентифікації з використанням відповідної бібліотеки підпису, що включає:

6.1) відправку бібліотекою запиту у ЦСК на формування позначки часу за протоколом TSP та отримання відповіді з ЦСК із сформованою позначкою;

6.2) формування ЕЦП з позначкою часу з використанням особистого ключа користувача ЦСК;

7) відправку користувачем запиту на ідентифікацію із підписаним даними серверу ідентифікації за методом POST протоколу HTTPS;

8) перевірку сервером ідентифікації підписаних даних ідентифікації від користувача з використанням бібліотеки підпису у вигляді модуля розширення PHP і мережного криптомодуля та прийняття рішення про успішність ідентифікації користувача, що включає:

8.1) відправку бібліотекою запиту у ЦСК на пошук та перевірку статусу сертифіката користувача за протоколом OCSP і отримання відповіді та завантаження з ЦСК поточних СВС і перевірку статусу сертифіката з використанням завантажених СВС;

8.2) перевірку ЕЦП з використанням перевіреного сертифіката особистого ключа користувача ЦСК;

9) відправку (у разі успішної ідентифікації) сервером ідентифікації користувачеві відповіді із перенаправленням браузера користувача на сторінку сервера прикладної системи, яка була вказана в якості зворотного посилання (**redirect_uri**) під час попереднього перенаправлення на сервер ідентифікації;

10) відправку користувачем (за результатом перенаправлення браузеру) запиту на завершення ідентифікації серверу прикладної системи за методом GET протоколу HTTP(S) на перенаправлене посилання виду:

```
GET
http(s)://url/redirect?code=code&
   state=state
```

Параметри запиту описані у табл. 2.2.2.

Таблиця 2.2.2 – Опис параметрів запиту користувача на завершення ідентифікації

Параметри	Опис
http(s)://url/redirect	Зворотнє посилання на сторінку web-сервера прикладної системи (**redirect_uri**)
code	Код авторизації
state	Значення, що надсилалось у запиті на кроці 3

11) обробку сервером прикладної системи запиту на завершення ідентифікації користувача, що включає:

11.1) відправку сервером прикладної системи запита серверу ідентифікації на отримання маркера доступу за кодом завершення ідентифікації (**code**) методом GET чи POST протоколу HTTPS виду:

```
GET / POST
https://id.gov.ua/get-access-token?grant_type=authorization_code&
   client_id= &
   client_secret= &
   code= &
   redirect_uri=https://url/redirect
```

11.2) обробку запиту та відправку сервером ідентифікації серверу прикладної системи відповіді з маркером доступу у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «access_token»:«»,
   «token_type»:«bearer»,
   «expires_in»:«»,
```

```
    «refresh_token»:«»,
    «user_id»:«»
}
```

Параметри відповіді описані у табл. 2.2.3.

Таблиця 2.2.3 – Опис параметрів відповіді серверу прикладної системи з маркером доступу

Параметри	Опис
access_token	Маркер доступу (значення маркеру наведене для прикладу)
token_type	Тип маркеру доступу (має фіксоване значення для застосування засобами ідентифікації – **bearer** – доступ за маркером для пред'явника)
expires_in	Час завершення дії маркеру доступу
user_id	Ідентифікатор ідентифікованого користувача за яким може бути отримана інформація про користувача

У тестовому сервері ідентифікації ідентифікатори ідентифікованих користувачів (**user_id**) зберігаються разом з інформацією з сертифікатів користувачів у тимчасовій базі даних (БД) і час завершення дії маркеру доступу (**expires_in**) вказує на термін існування відповідних записів у БД. У разі помилки обробки запиту відправляється структура у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
    «error»:«invalid_grant»,
    «error_description»:«»
}
```

Параметри відповіді описані у табл. 2.2.4.

Таблиця 2.2.4 – Опис параметрів помилки відповіді серверу прикладної системи з маркером доступу

Параметри	Опис
error	Тип помилки (значення наведене для прикладу)
error_description	Опис помилки (значення наведене для прикладу)

11.3) відправку сервером прикладної системи наступного запиту до сервера ідентифікації на отримання інформації про користувача за маркером доступу (**access_token**) методом GET чи POST протоколу HTTPS виду:

```
GET / POST
https://id.gov.ua/get-user-info?&access_token=access_token&
    user_id=36&
    fields=issuer,issuercn,serial,subject,subjectcn,locality,state,o,ou,title,lastname,
middlename,givenname,email,address,phone,dns,edrpoucode,drfocode&
    cert=
```

Параметри запиту описані у табл. 2.2.5.

Таблиця 2.2.5 – Опис параметрів запиту на отримання інформації про користувача сервером прикладної системи

Параметри	Опис
access_token	Маркер доступу
user_id	Ідентифікатор ідентифікованого користувача (значення наведене для прикладу)
fields	Назви полів сертифіката користувача, які запитуються. Якщо назви полів (**fields**) не вказані, то повертаються усі доступні поля сертифіката з інформацією про користувача (власника сертифіката) та видавника

	(ЦСК)
cert	Сертифікат протоколу розподілу ключів, на який буде зашифровано відповідь сервером ідентифікації, у форматі BASE64

11.4) обробка сервером ідентифікації запиту шляхом формування зашифрованої (з використанням бібліотеки підпису у вигляді модуля розширення PHP і мережного криптомодуля) відповіді з інформацією про ідентифікованого користувача у вигляді JSON-тексту виду:

```
Content-Type: application/json

{
   «auth_type»:«dig_sign»,
   «issuer»:«»,
   «issuercn»:«»,
   «serial»:«»,
   «subject»:«»,
   «subjectcn»:«»,
   «locality»:«»,
   «state»:«»,
   «o»:«»,
   «ou»:«»,
   «title»:«»,
   «lastname»:«»,
   «givenname»:«»,
   «middlename»:«»,
   «email»:«»,
   «address»:«»,
   «phone»:«»,
   «dns»:«»,
   «edrpoucode»:«»,
   «drfocode»:«»
}
```

Усі можливі поля сертифікату користувача, які повертає сервер ідентифікації після ідентифікації користувача (клієнта) системи через ЦСК (за ЕЦП) та з використанням паспорта громадянина України у формі ID-картки наведені у табл. 2.2.6.

Таблиця 2.2.6 - Усі можливі поля, які повертає сервер ідентифікації після ідентифікації через ЦСК та з використанням паспорта громадянина України у формі ID-картки.

Назва поля (одне із значень назв полів **fields**)	Опис вмісту поля
issuer	Реквізити видавника сертифіката (ЦСК)
issuercn	Загальне ім’я ЦСК
serial	Реєстраційний номер сертифіката у ЦСК
subject	Реквізити власника сертифіката (користувача)
subjectcn	Загальне ім’я користувача
locality	Місто (населений пункт) користувача
state	Область (регіон) користувача
o	Найменування організації користувача
ou	Назва підрозділу організації користувача
title	Посада користувача
givenname	Ім’я користувача
middlename	По батькові користувача
lastname	Прізвище користувача
email	Адреса ел. пошти (e-mail) користувача
address	Адреса (фізична) користувача
phone	Телефон користувача
dns	DNS-ім'я користувача

edrpoucode	Код ЄДРПОУ користувача
drfocode	Код ДРФО користувача

Параметри відповіді описані у табл. 2.2.7.

Таблиця 2.2.7 – Опис параметрів відповіді з інформацією про ідентифікованого користувача

Параметри	Опис
auth_type	Тип аутентифікації, що було обрано користувачем (можливі варіанти: **dig_sign**, **bank_id**, **mobile_id**)
issuer, **issuercn** та ін	Відповідні поля сертифіката користувача (значення полів наведені для прикладу)

Відповідь відправляється у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «encryptedUserInfo»:«»
}
```

У разі помилки обробки запиту відправляється структура у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «error»:«invalid_grant»,
   «error_description»:«»
}
```

Параметри відповіді описані у табл. 2.2.8.

Таблиця 2.2.8 – Опис параметрів помилки відповіді з інформацією про ідентифікованого користувача

Параметри	Опис
error	Тип помилки (значення наведене для прикладу)
error_description	Опис помилки (значення наведене для прикладу)

11.5) відправку сервером ідентифікації серверу прикладної системи зашифрованої відповіді з інформацією про ідентифікованого користувача;

11.6) отримання та розшифрування сервером прикладної системи відповіді з інформацією про користувача (клієнта) та прийняття рішення сервером прикладної системи про завершення ідентифікації;

12) відправку сервером прикладної системи відповіді користувачеві про завершення ідентифікації.

Засоби, які реалізують електронну ідентифікацію через центри сертифікації ключів та з використанням паспорта громадянина України у формі ID-картки, також підтримують можливість формування ЕЦП довільних даних для серверів та користувачів прикладних систем. При цьому безпосередньо використовуються засоби ЕЦП (бібліотеки підпису користувача ЦСК) на стороні користувача та сервера прикладної системи з використанням особистих ключів на носіях ключової інформації (НКІ) та паспорта громадянина України у формі ID-картки.

Структурно-функціональна схема засобів ЕЦП з використанням особистих ключів на НКІ та паспорта громадянина України у формі ID-картки наведена на рис. 2.2.

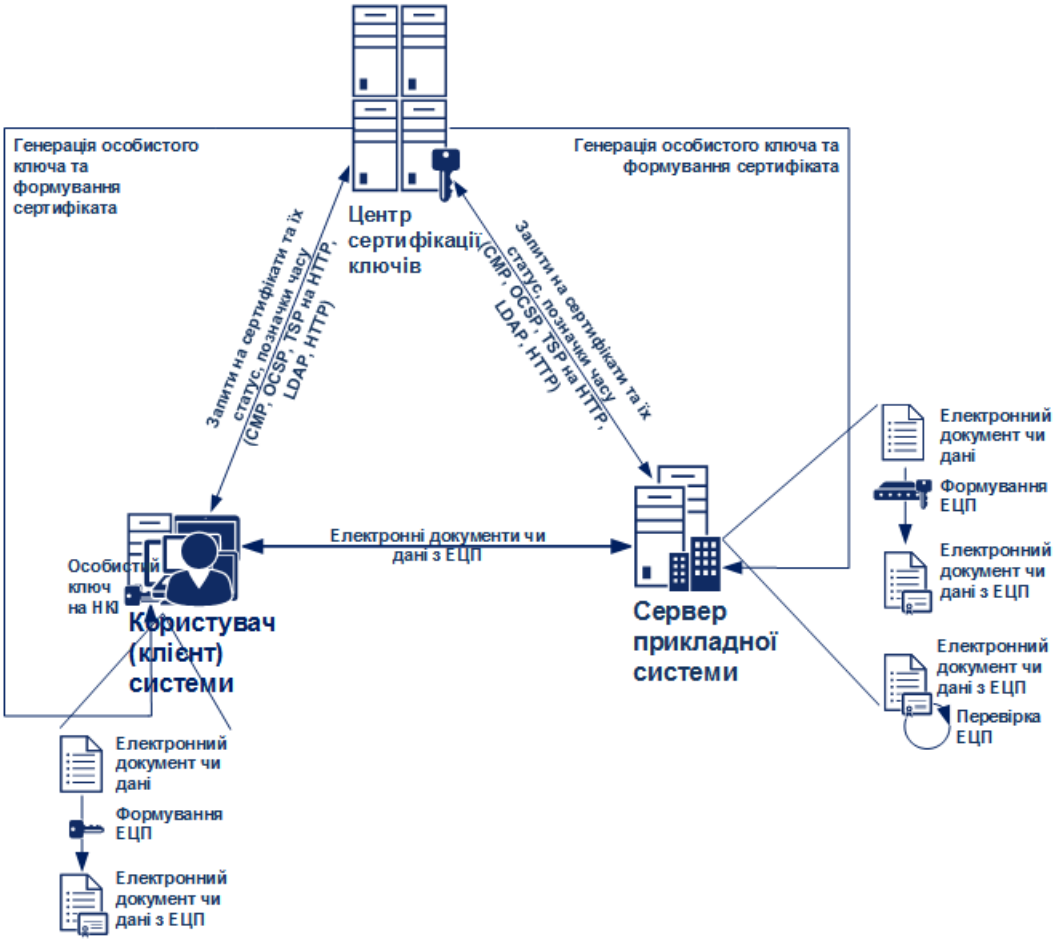

Рисунок 2.2 – Структурно-функціональна схема засобів ЕЦП з використанням особистих ключів на НКІ та паспорта громадянина України у формі ID-картки

2.3 Порядок електронної ідентифікації з використанням мобільного зв'язку (MobileID)

Структурно-функціональна схема електронної ідентифікації з використанням ресурсів мереж мобільного зв'язку (Mobile ID) наведено на рис. 2.3.

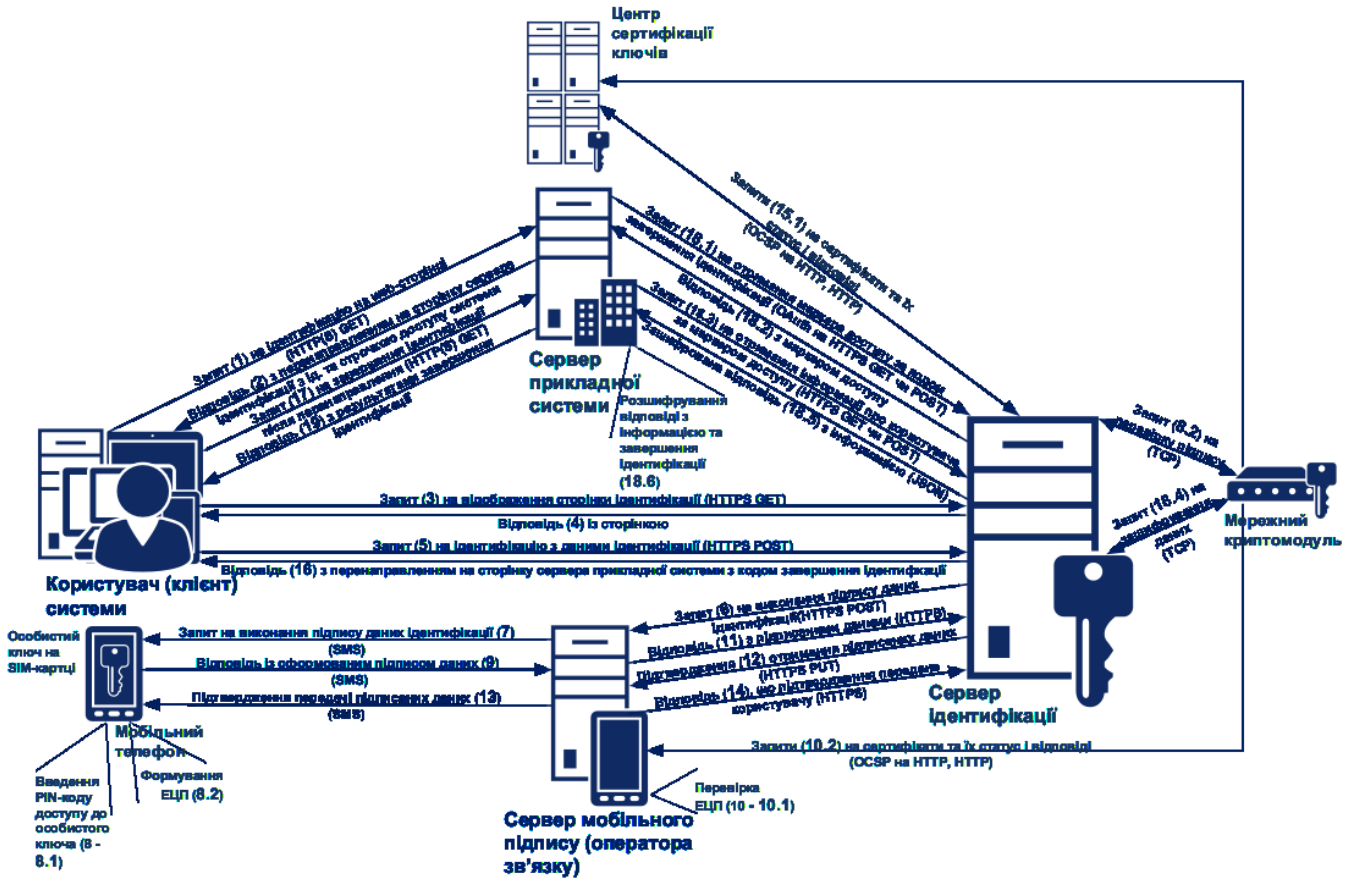

Рисунок 2.3 – Структурно-функціональна схема електронної ідентифікації з використанням ресурсів мереж мобільного зв'язку (Mobile ID)

Порядок взаємодії складових частин Системи під час ідентифікації користувача (клієнта) Системи на сервері прикладної системи з використанням ресурсів мереж мобільного зв'язку (Mobile ID) повинен включати:

1) відправку користувачем (клієнтом) запиту на ідентифікацію з web-браузера на web-сторінці web-сервера прикладної системи (натискання посилання або контекстна відправка запиту) за методом GET протоколу HTTP(S);

2) обробку запиту та відправку web-сервером прикладної системи користувачеві відповіді із перенаправленням браузера користувача на відповідну сторінку сервера ідентифікації (перенаправлене посилання);

3) відправку користувачем запиту на відображення відповідної сторінки серверу ідентифікації за методом GET протоколу HTTPS на перенаправлене посилання виду:

```
GET

https://id.gov.ua/?response_type=code&
    client_id=client_id&
    auth_type=dig_sign,bank_id,mobile_id&
    state=state&
    redirect_uri= http(s)://url/redirect
```

Параметри запиту описані у табл. 2.3.1.

Таблиця 2.3.1 – Опис параметрів запиту користувача серверу ідентифікації

Параметри	Опис
response_type	Повинен мати значення **code**

client_id	Ідентифікатор прикладної системи (значення наведене для прикладу)
auth_type	Параметр, що визначає можливі засоби ідентифікації (задається перелік необхідних засобів аутентифікації, значення наведене для прикладу)
state	Параметр, значення якого має бути повернуто при переадресації на адресу, вказану у значенні **redirect_uri** (значення наведене для прикладу)
redirect_uri	Зворотне посилання (URI) на web-сервер прикладної системи (значення посилання **http(s)://url/redirect** наведене для прикладу), на яке сервер ідентифікації перенаправить браузер користувача після виконання процедури ідентифікації

Зворотне посилання (**redirect_uri**) також може бути попередньо встановлене не сервері ідентифікації разом із ідентифікатором прикладної системи (**client_id)** та секретною строчкою доступу (**client_secret)** у реєстраційних даних відповідної прикладної системи. У цьому випадку сервер прикладної системи може не передавати зворотне посилання у запиті, а сервер ідентифікації буде брати його з реєстраційних даних прикладної системи;

4) обробку запиту та відправку сервером ідентифікації користувачеві відповіді із вмістом web-сторінки ідентифікації;

5) відправку користувачем запиту на ідентифікацію із даними мобільної ідентифікації (номером мобільного телефону, ідентифікатором оператора мобільного зв'язку та додаткових даних) за методом POST протоколу HTTPS;

6) відправку сервером ідентифікації на сервер мобільного підпису (сервер ЕЦП оператора зв'язку) запиту на підпис даних ідентифікації, де в якості параметрів передаються номер телефону користувача, дані для підпису, час відправки запиту та додаткові дані;

7) відправку сервером мобільного підпису на мобільний телефон користувача запиту у вигляді службового SMS-повідомленням на підпис даних ідентифікації;

8) формування користувачем ЕЦП - підпис даних ідентифікації з використанням особистого ключа у SIM-картці, яка встановлена у мобільному телефоні користувача:

8.1) введення користувачем на своєму мобільному телефоні PIN-коду доступу до особистого ключа підпису у SIM-картці при отриманні службового SMS-повідомлення;

8.2) формування ЕЦП з використанням особистого ключа користувача ЦСК безпосередньо у SIM-картці;

9) відправку користувачем відповіді (службовим SMS-повідомленням) із сформованим ЕЦП на сервер мобільного підпису;

10) перевірку сервером мобільного підпису підписаних даних від користувача та прийняття рішення про успішність виконання підпису:

10.1) відправку сервером мобільного підпису запиту у ЦСК на пошук та перевірку статусу сертифіката користувача за протоколом OCSP і отримання відповіді та завантаження з ЦСК поточних СВС і перевірку статусу сертифіката з використанням завантажених СВС;

10.2) перевірку ЕЦП даних ідентифікації з використанням перевіреного сертифіката особистого ключа користувача ЦСК;

11) відправку (у разі успішної перевірки підпису) сервером мобільного підпису серверу ідентифікації відповіді із підписаними даними, а у разі виникнення збою при виконанні пп. 7-10 відправляється відповідне повідомлення про збій;

12) відправку сервером ідентифікації на сервер мобільного підпису підтвердження отримання підписаних даних ідентифікації;

13) відправку сервером мобільного підпису на мобільний телефон користувача службового SMS-повідомлення з підтвердженням отримання сервером ідентифікації підписаних даних;

14) відправку сервером мобільного підпису серверу ідентифікації повідомлення про успішну передачу підтвердження;

15) перевірку сервером ідентифікації підписаних даних ідентифікації від користувача з використанням бібліотеки підпису у вигляді модуля розширення PHP і мережного криптомодуля та прийняття рішення про успішність ідентифікації користувача, що включає:

15.1) відправку бібліотекою запиту у ЦСК на пошук та перевірку статусу сертифіката користувача за протоколом OCSP і отримання відповіді та завантаження з ЦСК поточних СВС і перевірку статусу сертифіката з використанням завантажених СВС;

15.2) перевірку ЕЦП з використанням перевіреного сертифіката особистого ключа користувача ЦСК;

16) відправку (у разі успішної ідентифікації) сервером ідентифікації користувачеві відповіді із перенаправленням браузера користувача на сторінку сервера прикладної системи, яка була вказана в якості зворотного посилання (**redirect_uri**) під час попереднього перенаправлення на сервер ідентифікації;

17) відправку користувачем (за результатом перенаправлення браузеру) запиту на завершення ідентифікації серверу прикладної системи за методом GET протоколу HTTP(S) на перенаправлене посилання виду:

```
GET

http(s)://url/redirect?code=code&
    state=state
```

Параметри запиту описані у табл. 2.3.2.

Таблиця 2.3.2 – Опис параметрів запиту користувача на завершення ідентифікації

Параметри	Опис
http(s)://url/redirect	Зворотне посилання на сторінку web-сервера прикладної системи (**redirect_uri**)
code	Код авторизації
state	Значення, що надсилалось у запиті на кроці 3

18) обробку сервером прикладної системи запиту на завершення ідентифікації користувача, що включає:

18.1) відправку сервером прикладної системи запита серверу ідентифікації на отримання маркера доступу за кодом завершення ідентифікації (**code**) методом GET чи POST протоколу HTTPS виду:

```
GET / POST

https://id.gov.ua/get-access-token?grant_type=authorization_code&
    client_id=client_id&
    client_secret=client_secret&
    code=&
    redirect_uri=https://url/redirect
```

18.2) обробку запиту та відправку сервером ідентифікації серверу прикладної системи відповіді з маркером доступу у вигляді JSON-тексту виду:

```
Content-Type: application/json

{
    «access_token»:«»,
    «token_type»:«bearer»,
    «expires_in»:«»,
    «refresh_token»:«»,
    «user_id»:«»
}
```

Параметри відповіді описані у табл. 2.3.3.

Таблиця 2.3.3 – Опис параметрів відповіді серверу прикладної системи з маркером доступу

Параметри	Опис
access_token	Маркер доступу (значення маркеру наведене для прикладу)
token_type	Тип маркеру доступу (має фіксоване значення для застосування засобами ідентифікації - **bearer** - доступ за маркером для пред'явника)
expires_in	Час завершення дії маркеру доступу
user_id	Ідентифікатор ідентифікованого користувача за яким може бути отримана інформація про користувача

У тестовому сервері ідентифікації ідентифікатори ідентифікованих користувачів (**user_id**) зберігаються разом з інформацією з сертифікатів користувачів у тимчасовій базі даних (БД) і час завершення дії маркеру доступу (**expires_in**) вказує на термін існування відповідних записів у БД. У разі помилки обробки запиту відправляється структура у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «error»:«invalid_grant»,
   «error_description»:«»
}
```

Параметри відповіді описані у табл. 2.3.4.

Таблиця 2.3.4 - Опис параметрів помилки відповіді серверу прикладної системи з маркером доступу

Параметри	Опис
error	Тип помилки (значення наведене для прикладу)
error_description	Опис помилки (значення наведене для прикладу)

18.3) відправку сервером прикладної системи наступного запиту до сервера ідентифікації на отримання інформації про користувача за маркером доступу (**access_token**) методом GET чи POST протоколу HTTPS виду:

```
GET / POST
https://id.gov.ua/get-user-info?&access_token=&
   user_id=36&
   fields=issuer,issuercn,serial,subject,subjectcn,locality,
state,o,ou,title,surname,givenname,email,address,phone,dns,edrpoucode,drfocode&
   cert=
```

Параметри запиту описані у табл. 2.3.5.

Таблиця 2.3.5 - Опис параметрів запиту на отримання інформації про користувача сервером прикладної системи

Параметри	Опис
access_token	Маркер доступу
user_id	Ідентифікатор ідентифікованого користувача (значення наведене для прикладу)
fields	Назви полів сертифіката користувача, які запитуються. Якщо назви полів (**fields**) не вказані, то повертаються усі доступні поля сертифіката з інформацією про користувача (власника сертифіката) та видавника (ЦСК)
cert	Сертифікат протоколу розподілу ключів, на який буде зашифровано відповідь сервером ідентифікації, у форматі BASE64

18.4) обробка сервером ідентифікації запиту шляхом формування зашифрованої (з використанням бібліотеки підпису у вигляді модуля розширення PHP і мережного криптомодуля) відповіді з інформацією про ідентифікованого користувача у вигляді JSON-тексту виду:

```
Content-Type: application/json

{
   «auth_type»:«dig_sign»,
   «issuer»:«»,
   «issuercn»:«»,
   «serial»:«»,
   «subject»:«»,
   «subjectcn»:«»,
   «locality»:«»,
   «state»:«»,
   «o»:«»,
   «ou»:«»,
   «title»:«»,
   «lastname»:«»,
   «givenname»:«»,
   «middlename»:«»,
   «email»:«»,
   «address»:«»,
   «phone»:«»,
   «dns»:«»,
   «edrpoucode»:«»,
   «drfocode»:«»
}
```

Усі можливі поля сертифікату користувача, які повертає сервер ідентифікації після ідентифікації користувача (клієнта) системи через операторів мобільного зв'язку (MobileID) за мобільним ЕЦП наведені у табл. 2.3.6.

Таблиця 2.3.6 - Усі можливі поля, які повертає сервер ідентифікації після ідентифікації через операторів мобільного зв'язку (MobileID).

Назва поля (одне із значень назв полів **fields**)	Опис вмісту поля
issuer	Реквізити видавника сертифіката (ЦСК)
issuercn	Загальне ім’я ЦСК
serial	Реєстраційний номер сертифіката у ЦСК
subject	Реквізити власника сертифіката (користувача)
subjectcn	Загальне ім’я користувача
locality	Місто (населений пункт) користувача
state	Область (регіон) користувача
o	Найменування організації користувача
ou	Назва підрозділу організації користувача
title	Посада користувача
givenname	Ім’я користувача
middlename	По батькові користувача
lastname	Прізвище користувача
email	Адреса ел. пошти (e-mail) користувача
address	Адреса (фізична) користувача
phone	Телефон користувача
dns	DNS-ім'я користувача
edrpoucode	Код ЄДРПОУ користувача
drfocode	Код ДРФО користувача

Параметри відповіді описані у табл. 2.3.7.

Таблиця 2.3.7 – Опис параметрів відповіді з інформацією про ідентифікованого користувача

Параметри	Опис
auth_type	Тип аутентифікації, що було обрано користувачем (можливі варіанти: **dig_sign**, **bank_id**, **mobile_id**)
issuer, **issuercn** та ін	Відповідні поля сертифіката користувача (значення полів наведені для прикладу)

Відповідь відправляється у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «encryptedUserInfo»:«»
}
```

У разі помилки обробки запиту відправляється структура у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «error»:«invalid_grant»,
   «error_description»:«»
}
```

Параметри відповіді описані у табл. 2.3.8.

Таблиця 2.3.8 – Опис параметрів помилки відповіді з інформацією про ідентифікованого користувача

Параметри	Опис
error	Тип помилки (значення наведене для прикладу)
error_description	Опис помилки (значення наведене для прикладу)

18.5) відправку сервером ідентифікації серверу прикладної системи зашифрованої відповіді з інформацією про ідентифікованого користувача;

18.6) отримання та розшифрування сервером прикладної системи відповіді з інформацією про користувача (клієнта) та прийняття рішення сервером прикладної системи про завершення ідентифікації;

19) відправку сервером прикладної системи відповіді користувачеві про завершення ідентифікації.

Засоби, які реалізують електронну ідентифікацію з використанням ресурів мереж мобільного зв'язку (MobileID), також підтримують можливість формування ЕЦП довільних даних для серверів та користувачів прикладних систем. При цьому використовуються засоби ЕЦП операторів мобільного зв'язку (MobileID) з особистими ключами у SIM-картках мобільних телефонів та засоби ЕЦП (бібліотеки підпису користувача ЦСК) на стороні сервера прикладної системи. Взаємодія сервера прикладної системи під час формування ЕЦП у SIM-картці мобільного телефону здійснюється через сервер мобільного підпису (оператора з'язку).

Структурно-функціональна схема засобів ЕЦП операторів мобільного зв'язку (MobileID) наведена на рис. 2.4.

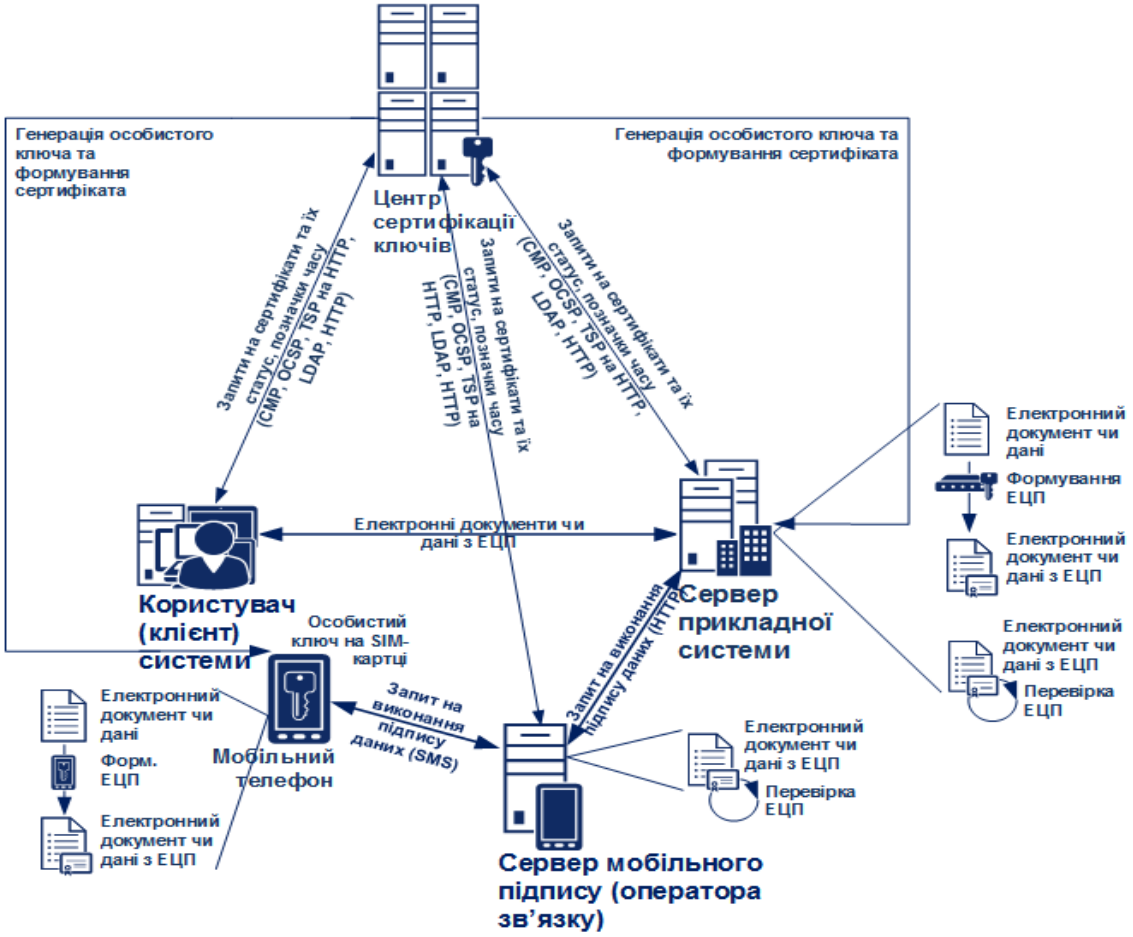

Рисунок 2.4 - Структурно-функціональна схема засобів ЕЦП операторів мобільного зв'язку (MobileID)

2.4 Порядок електронної ідентифікації банківських установ (BankID)

Структурно-функціональна схема електронної ідентифікації банківських установ (BankID) наведено на рис. 2.5.

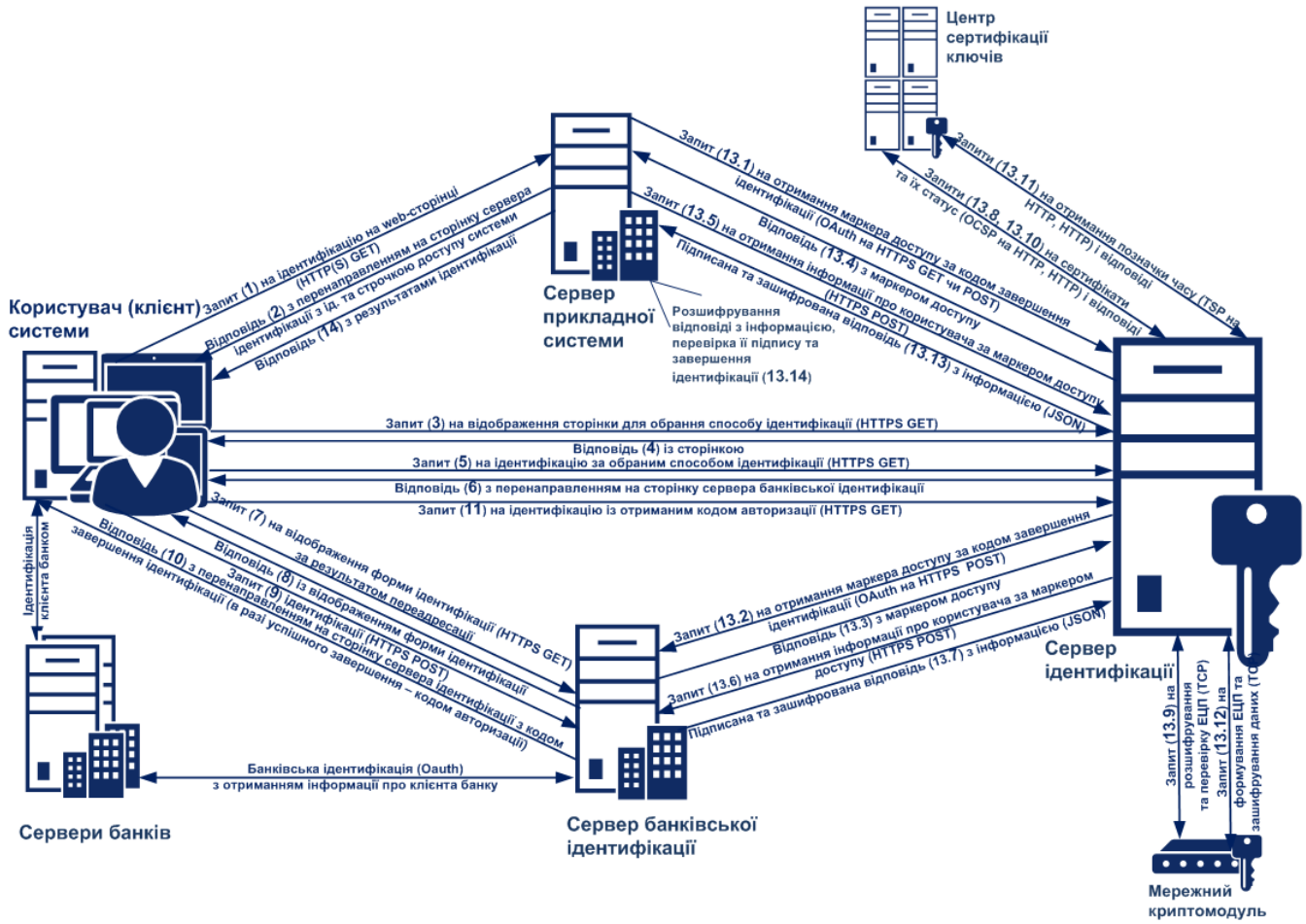

Рисунок 2.5 – Структурно-функціональна схема електронної ідентифікації банківських установ (BankID)

Порядок взаємодії складових частин Системи під час ідентифікації користувача (клієнта) Системи на сервері прикладної системи з використанням банківських установ (BankID) повинен включати:

1) відправку користувачем (клієнтом) запиту на ідентифікацію з web-браузера на web-сторінці web-сервера прикладної системи (натискання посилання або контекстна відправка запиту) за методом GET протоколу HTTP(S);
2) обробку запиту та відправку web-сервером прикладної системи користувачеві відповіді із перенаправленням браузера користувача на відповідну сторінку сервера ідентифікації (перенаправлене посилання);
3) відправку користувачем запиту на відображення відповідної сторінки серверу ідентифікації за методом GET протоколу HTTPS на перенаправлене посилання виду:

```
GET

https://id.gov.ua/?response_type=code&
    client_id=client_id&
    auth_type=dig_sign,bank_id,mobile_id&
    state=state&
    redirect_uri= http(s)://url/redirect
```

Параметри запиту описані у табл. 2.4.1.

Таблиця 2.4.1 – Опис параметрів запиту користувача серверу ідентифікації

Параметри	Опис
response_type	Повинен мати значення **code**
client_id	Ідентифікатор прикладної системи (значення наведене для прикладу)
auth_type	Параметр, що визначає можливі засоби ідентифікації (задається перелік необхідних засобів аутентифікації, значення наведене для прикладу)
state	Параметр, значення якого має бути повернуто при переадресації на адресу, вказану у значенні **redirect_uri** (значення наведене для прикладу)
redirect_uri	Зворотне посилання (URI) на web-сервер прикладної системи (значення посилання **http(s)://url/redirect** наведене для прикладу), на яке сервер ідентифікації перенаправить браузер користувача після виконання процедури ідентифікації

Зворотне посилання (**redirect_uri**) також може бути попередньо встановлене не сервері ідентифікації разом із ідентифікатором прикладної системи (**client_id)** та секретною строчкою доступу (**client_secret)** у реєстраційних даних відповідної прикладної системи. У цьому випадку сервер прикладної системи може не передавати зворотне посилання у запиті, а сервер ідентифікації буде брати його з реєстраційних даних прикладної системи;

4) обробку запиту та відправку сервером ідентифікації користувачеві відповіді із вмістом web-сторінки ідентифікації;
5) відправку користувачем запиту на банківську ідентифікацію за методом GET протоколу HTTPS;
6) відправку користувачем запиту на відображення відповідної сторінки серверу банківської ідентифікації за методом GET протоколу HTTPS на перенаправлене посилання виду:

```
GET

https://id.gov.ua/?response_type=code&
    client_id=client_id&
    redirect_uri=http(s)://url/redirect&
    state=
```

Параметри запиту описані у табл. 2.4.2.

Таблиця 2.4.2 – Опис параметрів запиту користувача на сервер банківської ідентифікації

Параметри	Опис
client_id	Ідентифікатор прикладної системи
redirect_uri	Зворотне посилання (URI) на web-сервер ідентифікації (значення посилання **http(s)://url/redirect** наведене для прикладу), на яке сервер банківської ідентифікації перенаправить браузер користувача після виконання процедури ідентифікації
state	Параметр, значення якого має бути повернуто сервером банківської ідентифікації при переадресації на адресу сервера ідентифікації, вказану у значенні **callback_url**. Використовується для уникнення CSRF атак

Зворотне посилання (**redirect_uri**) також може бути попередньо встановлене на сервері банківської ідентифікації разом із ідентифікатором сервера ідентифікації (**client_id)** та секретною строчкою доступу (**client_secret)** у реєстраційних даних відповідного сервера ідентифікації.

7) запит на відображення форми ідентифікації сервером банківської ідентифікації (за результатом переадресації);
8) формування форми ідентифікації сервером банківської ідентифікації та відправка користувачу;
9) заповнення та відправка користувачем форми ідентифікації на web-сторінці сервера банківської ідентифікації;

10) обробку запиту та відправку сервером банківської ідентифікації користувачеві відповіді із перенаправленням браузера користувача на відповідну сторінку сервера ідентифікації (перенаправлене посилання);
11) відправку користувачем запиту на відображення відповідної сторінки серверу ідентифікації за методом GET протоколу HTTPS на перенаправлене посилання виду:

```
GET
http(s)://url/redirect?code=code&
    state=state
```

Параметри запиту описані у табл. 2.4.3.

Таблиця 2.4.3 – Опис параметрів запиту користувача на сервер ідентифікації

Параметри	Опис
http(s)://url/redirect	Зворотнє посилання на сторінку web-сервера ідентифікації (**redirect_uri**)
code	Код авторизації (authorization code)
state	Значення, що використовувалось при відповіді з кодом авторизаці

Якщо під час запиту виникали помилки, то:

- або сервер банківської ідентифікації не вдалося ідентифікувати на сервері банку (зокрема, не зареєстрований на стороні банку, не співпадає значення параметру **client_id**) або некоректний запит. В такому випадку опис помилки буде відображено на web-сторінці сервера банку;
- або користувача вдалося ідентифікувати на ресурсі сервера банку, проте сталася інша помилка – буде виконано переадресацію на адресу параметра **redirect_uri** з наступними параметрами у тілі запиту (body) в JSON-форматі.

У разі помилки разі помилки обробки запиту відправляється структура у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
    «error»:«invalid_grant»,
    «error_description»:«»,
    «state»: «»
}
```

Параметри відповіді описані у табл. 2.4.4.

Таблиця 2.4.4 – Опис параметрів відповіді у разі виникнення помилки

Параметри	Опис
error	Один з визначених кодів помилки згідно протоколу OAuth. Зокрема: **invalid_request, unauthorized_client**, **access_denied, unsupported_response_type, invalid_scope, server_error, temporarily_unavailable**
error_description	Можливий текстовий опис помилки, деталізація для розробників
state	Значення, що використовувалось при відповіді з кодом авторизації

12) відправку сервером ідентифікації запиту на завершення ідентифікації серверу прикладної системи за методом GET протоколу HTTP(S) на перенаправлене посилання виду:

```
GET
http(s)://url/redirect?code=code&
    state=state
```

Параметри запиту описані у табл. 2.4.5.

Таблиця 2.4.5 – Опис параметрів запиту сервера ідентифікації на завершення ідентифікації

Параметри	Опис
http(s)://url/redirect	Зворотнє посилання на сторінку web-сервера прикладної системи (**redirect_uri**)
code	Код авторизації
state	Значення, що надсилалось у запиті на кроці 3

13) обробку сервером прикладної системи запиту на завершення ідентифікації користувача, що включає:

13.1) відправку сервером прикладної системи запита серверу ідентифікації на отримання маркера доступу за кодом завершення ідентифікації (**code**) методом GET чи POST протоколу HTTPS виду:

```
GET / POST

https://id.gov.ua/get-access-token?grant_type=authorization_code&
   client_id=client_id&
   client_secret=client_secret&
   code=&
   redirect_uri=https://url/redirect
```

13.2) відправку сервером ідентифікації запита серверу банківської ідентифікації на отримання маркера доступу (**access_token**). Запит методом POST виду:

```
POST

https://url/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
```

Параметри запиту описані у табл. 2.4.6.

Таблиця 2.4.6 – Опис параметрів запиту на отримання маркера доступу сервером ідентифікації

Параметри	Опис
grant_type	Тип запиту який повинен мати значення «**authorization_code**». (У іншому випадку, запит на продовження дії маркеру доступу (**access_token**), значення буде «**refresh_token**»)
code	Код авторизації (**authorization code**), отриманий на попередньому кроці
callback_url	Адреса сервера ідентифікації, у даному випадку використовується для переадресації у разі виникнення помилок при отриманні маркера доступу (**access_token**)

13.3) відповідь сервера банківської ідентифікації із маркером доступу, у вигляді JSON-структури:

```
Content-Type: application/json

{
   «token_type»:«bearer»,
   «access_token»:«»,
   «expires_in»:«»,
   «refresh_token»:«»
}
```

У разі виникнення помилок оброблення запиту, відповідний сервер банку переадресовує користувача на адресу callback_url і вказує нижчезазначені параметри і значення, що спричинили відмову. Параметри із значеннями передаються у тілі запиту (body) у JSON-форматі. У разі помилки разі помилки обробки запиту відправляється структура у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «error»:«invalid_grant»,
   «error_description»:«»,
   «state»: «»
}
```

Параметри відповіді описані у табл. 2.4.7.

Таблиця 2.4.7 – Опис параметрів відповіді у разі виникнення помилки

Параметри	Опис
error	Один з визначених кодів помилки згідно протоколу OAuth. Зокрема: **invalid_request, unauthorized_client**, **access_denied, unsupported_response_type, invalid_scope, server_error, temporarily_unavailable**
error_description	Можливий текстовий опис помилки, деталізація для розробників
state	Значення, що використовувалось при відповіді з кодом авторизації

13.4) обробку запиту та відправку сервером ідентифікації серверу прикладної системи відповіді з маркером доступу у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «access_token»:«»,
   «token_type»:«bearer»,
   «expires_in»:«»,
   «refresh_token»:«»,
   «user_id»:«»
}
```

Параметри відповіді описані у табл. 2.4.8.

Таблиця 2.4.8 – Опис параметрів відповіді серверу прикладної системи з маркером доступу

Параметри	Опис
access_token	Маркер доступу (значення маркеру наведене для прикладу)
token_type	Тип маркеру доступу (має фіксоване значення для застосування засобами ідентифікації – **bearer** – доступ за маркером для пред'явника)
expires_in	Час завершення дії маркеру доступу
user_id	Ідентифікатор ідентифікованого користувача за яким може бути отримана інформація про користувача

У тестовому сервері ідентифікації ідентифікатори ідентифікованих користувачів (user_id) зберігаються разом з інформацією з сертифікатів користувачів у тимчасовій базі даних (БД) і час завершення дії маркеру доступу (expires_in) вказує на термін існування відповідних записів у БД. У разі помилки обробки запиту відправляється структура у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «error»:«invalid_grant»,
   «error_description»:«»
}
```

Параметри відповіді описані у табл. 2.4.9.

Таблиця 2.4.9 – Опис параметрів помилки відповіді серверу прикладної системи

Параметри	Опис
error	Тип помилки (значення наведене для прикладу)
error_description	Опис помилки (значення наведене для прикладу)

13.5) відправку сервером прикладної системи наступного запиту до сервера ідентифікації на отримання інформації про користувача за маркером доступу (**access_token**) та надання під час запиту сертифіката протоколу розподілу для направленого шифрування, методом GET чи POST протоколу HTTPS виду:

```
GET / POST
https://id.gov.ua/get-user-info?&access_token=&
   user_id=36&
   fields=issuer,issuercn,serial,subject,subjectcn,locality,
state,o,ou,title,surname,givenname,email,address,phone,dns,edrpoucode,drfocode&
   cert=
```

Надання даних відбувається на підставі маркеру доступу (access_token), отриманого у ході авторизації (згідно попереднього пункту). Маркер доступу передається в заголовку запиту (headers) у вигляді:

```
Authorization: «Bearer access_token»
```

Параметри запиту описані у табл. 2.4.10.

Таблиця 2.4.10 – Опис параметрів запиту на отримання інформації про користувача сервером прикладної системи

Параметри	Опис
access_token	Маркер доступу
user_id	Ідентифікатор ідентифікованого користувача (значення наведене для прикладу)
fields	Назви полів сертифіката користувача, які запитуються. Якщо назви полів (**fields**) не вказані, то повертаються усі доступні поля сертифіката з інформацією про користувача (власника сертифіката) та видавника (ЦСК)
cert	Сертифікат протоколу розподілу ключів, на який буде зашифровано відповідь сервером ідентифікації, у форматі BASE64

13.6) запит сервером ідентифікації даних користувача. Надання під час запиту сертифіката шифрування.

Надання даних відбувається на підставі маркеру доступу (**access_token**), отриманого у ході авторизації (згідно попереднього пункту). Маркер доступу передається в заголовку запиту (**headers**) у вигляді:

```
Authorization: «Bearer access_token»
```

Сервер ідентифікації, в запиті до сервера банківської ідентифікації, повинен вказати, який саме набір даних по клієнту потрібно передати у відповіді, а також надати свій сертифікат шифрування в форматі base64. Сервер банківської ідентифікації здійснює запит до сервера банку, у якому в свою чергу зазначає перелік необхідних даних та надає сертифікат шифрування сервера ідентифікації, для якого здійснюється автентифікація клієнта. Сертифікат шифрування передається в атрибуті «**cert**» у форматі BASE64.

Перелік необхідних даних вказується згідно допустимих полів у вигляді JSON-об'єкту в тілі запиту (**body**). Якщо якесь із полів буде відсутнє зі сторони сервера ідентифікації, то заказане поле повертається пустим.

Приклад JSON-об'єкту на запит персональних даних:

```
{
   «type»:«physical»,
   «cert»:«»,
   «fields»:[
      «firstName»,
      «middleName»,
      «lastName»,
      «phone»,
      «inn»,
      «birthDay»
   ],
   «addresses»:[
      {
         «type»:«factual»,
         «fields»:[«country»,«state»,«area»,«city»,«street»,«houseNo»,«flatNo»]
      }
   ]
}
```

13.7) обробка сервером банківської ідентифікації запиту шляхом формування, підпису та зашифрування відповіді з інформацією про ідентифікованого користувача у вигляді JSON-тексту виду:

```
{
   «state»:«ok»,
   «cert»:«»,
  «customerCrypto»:«»
}
```

що містить JSON-об'єкт **«customer»** з персональними даними користувача у вигляді:

```
«customer»:{
   «type»:«physical»,
   «inn»:«»,
   «sex»:«»,
   «email»:«»,
   «birthDay»:«»,
   «firstName»:«»,
```

```
    «lastName»:«»,
    «middleName»:«»,
    «phone»: «»,
    «addresses»:[
        {
            «type»:«factual»,
            «country»:«»,
             «state»:«»,
            «city»:«»,
            «street»:«»,
            «houseNo»:«»,
            «flatNo»:«»
        },
    ],
}
```

Значення **physical,** наведені в якості прикладу.

Усі можливі поля з інформацією про користувача, які повертає сервер ідентифікації після ідентифікації користувача (клієнта) системи через банківські установи (BankID) наведені у табл. 2.4.11.

Таблиця 2.4.11 - Усі можливі поля, які повертає сервер ідентифікації після ідентифікації через банківські установи (BankID).

Назва структури	Назва поля (одне із значень назв полів структури)	Опис вмісту поля
	state	
	cert	Сертифікат шифрування (у форматі BASE64) відправника даних
	customerCrypto	Містить зашифровану структуру **customer** (зашифровані дані у форматі BASE64)
customer	**lastName**	Прізвище
	firstName	Ім’я
	middleName	По батькові
	phone	Телефон користувача
	inn	Ідентифікаціний код користувача
	birthDay	Дата народження
	sex	Стать
	email	Адреса ел. пошти (e-mail)
	addresses	Містить структуру **addresses**
addresses	**type**	Тип адреси, допустимі значення: **factual** - фактична адреса проживання; **birth** - адреса місця народження; **juridical** - адреса реєстрації (штамп в паспорті).
	country	Країна
	state	Область
	area	Район
	city	Місто
	street	Вулиця
	houseNo	Номер будинку

	flatNo	Номер квартири

У разі помилки разі помилки обробки запиту відправляється структура у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «error»:«invalid_grant»,
   «error_description»:«»
}
```

Параметри відповіді описані у табл. 2.4.12.

Таблиця 2.4.12 – Опис параметрів помилки

Параметри	Опис
error	Тип помилки (значення наведене для прикладу)
error_description	Опис помилки (значення наведене для прикладу)

13.8) відправка сервером ідентифікації запиту у ЦСК на пошук та перевірку статусу сертифіката відправника (сервера банківської ідентифікації) за протоколом OCSP і отримання відповіді та завантаження з ЦСК поточних СВС та/або перевірку статусу сертифіката з використанням завантажених СВС/OCSP-відповіді;

13.9) відправка запиту щодо розшифрування та перевірки ЕЦП інформації про користувача мережному криптомодулю та отримання відповіді щодо з розшифрованою інформацією;

13.10) формування сервером ідентифікації запиту на отримання статусу сертифіката сервера прикладної системи до ЦСК та отримання відповіді;

13.11) формування запиту на отримання позначки часу до ЦСК та отримання відповіді із позначкою часу.

13.12) обробка сервером ідентифікації запиту шляхом формування, підпису та зашифрування (з використанням бібліотеки підпису у вигляді модуля розширення PHP і мережного криптомодуля) відповіді з інформацією про ідентифікованого користувача у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «auth_type»:«bank_id»,
   «issuer»:«»,
   «issuercn»:«»,
   «serial»:«»,
   «subject»:«»,
   «subjectcn»:«»,
   «locality»:«»,
   «state»:«»,
   «o»:«»,
   «ou»:«»,
   «title»:«»,
   «lastname»:«»,
   «givenname»:«»,
   «middlename»:«»,
   «email»:«»,
   «address»:«»,
   «phone»:«»,
   «dns»:«»,
   «edrpoucode»:«»,
   «drfocode»:«»
}
```

Усі можливі поля сертифікату користувача, які повертає сервер ідентифікації після ідентифікації користувача (клієнта) системи через банківські установи (BankID) наведені у табл. 2.4.13.

Таблиця 2.4.13 - Усі можливі поля, які повертає сервер ідентифікації після ідентифікації через банківські установи (BankID).

Назва поля (одне із значень назв полів **fields**)	Опис вмісту поля
issuer	Реквізити видавника сертифіката (ЦСК)
issuercn	Загальне ім'я ЦСК
serial	Реєстраційний номер сертифіката у ЦСК
subject	Реквізити власника сертифіката (користувача)
subjectcn	Загальне ім'я користувача
locality	Місто (населений пункт) користувача
state	Область (регіон) користувача
o	Найменування організації користувача
ou	Назва підрозділу організації користувача
title	Посада користувача
givenname	Ім'я користувача
middlename	По батькові користувача
lastname	Прізвище користувача
email	Адреса ел. пошти (e-mail) користувача
address	Адреса (фізична) користувача
phone	Телефон користувача
dns	DNS-ім'я користувача
edrpoucode	Код ЄДРПОУ користувача
drfocode	Код ДРФО користувача

Параметри відповіді описані у табл. 2.4.14.

Таблиця 2.4.14 – Опис параметрів відповіді з інформацією про ідентифікованого користувача

Параметри	Опис
auth_type	Тип аутентифікації, що було обрано користувачем (можливі варіанти: **dig_sign**, **bank_id**, **mobile_id**)
issuer, **issuercn** та ін	Відповідні поля даних про користувача (значення полів наведені для прикладу)

Всі дані про адресу вносяться до одного поля **address.**

Відповідь відправляється у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «encryptedUserInfo»:«»
}
```

У разі помилки обробки запиту відправляється структура у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «error»:«invalid_grant»,
   «error_description»:«»
}
```

Параметри відповіді описані у табл. 2.4.15.

Таблиця 2.4.15 – Опис параметрів помилки відповіді з інформацією про ідентифікованого користувача

Параметри	Опис
error	Тип помилки (значення наведене для прикладу)
error_description	Опис помилки (значення наведене для прикладу)

13.13) відправку сервером ідентифікації серверу прикладної системи зашифрованої та підписаної відповіді з інформацією про ідентифікованого користувача;

13.14) отримання, розшифрування та перевірка ЕЦП сервером прикладної системи відповіді з інформацією про користувача (клієнта) та прийняття рішення сервером прикладної системи про завершення ідентифікації;

14) відправку сервером прикладної системи відповіді користувачеві про завершення ідентифікації.

Для всіх подій у Системі, пов'язаних із взаємодією з системою ідентифікації BankID, здійснюється їх реєстрація шляхом ведення журналу аудиту. Усі записи в журналах аудиту містять опис події, дату та час події, а також забезпечувати ідентифікацію суб'єкта, що ініціював подію. Журнали аудиту мають захист від несанкціонованого доступу, модифікації та знищення (руйнування).

Взаємодія Системи з системою ідентифікації BankID забезпечує взаємну ідентифікацію та автентифікацію систем з використанням криптографічного протоколу TLS (Transport Layer Security). Для узгодження сеансових ключів використовуються протоколи Діффі-Геллмана (в простому полі – DHE та в групі точок еліптичної кривої ECDHE). Довжина відкритого ключа для протоколу Діффі-Геллмана в простому полі DH є не меншою 2048 біт. Довжина відкритого ключа для протоколу Діффі-Геллмана в групі точок еліптичної кривої ECDHE є не меншою 256 біт. Для шифрування інформації використовуються симетричні криптографічні алгоритми з довжиною ключа не менше 128 біт.

Банк (система банку) перед передаванням електронної анкети з інформацією про користувача (клієнта) через систему BankID послідовно виконує наступні операції:

– накладає на цю електронну анкету електронний цифровий підпис з використанням формату "ЕЦП з повним набором даних перевірки" (CAdES-X Long), що прирівнюється до печатки;

– шифрує підписану електронну анкету з використанням посиленого сертифікату шифрування того абонента-надавача послуг, якому передає електронну анкету.

Накладання електронного цифрового підпису на електронну анкету здійснюється відповідно до Вимог до формату підписаних даних, які затверджені наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.08.2012 р. № 1236/5/453 та зареєстровані в Міністерстві юстиції України 20.08.2012 р. за № 1401/21713 (зі змінами).

Шифрування/розшифрування електронної анкети відбувається згідно алгоритмів та правил, визначених Вимогами до форматів криптографічних повідомлень, які затверджені наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 р. № 739.

3 ПОРЯДОК ЗДІЙСНЕННЯ ОКРЕМИХ ЗАПИТІВ

3.1 Запит на подовження дії маркеру доступу

Запит складається з таких кроків:

1. відправку сервером прикладної системи запита серверу ідентифікації на подовження дії маркера доступу за маркером подовження дії маркеру доступу (**refresh_token**) методом GET чи POST протоколу HTTPS виду:

```
GET / POST
https://id.gov.ua/get-refresh-token?grant_type=refresh_token&
   client_id= &
   client_secret= &
   refresh_token=
```

2. обробку запиту та відправку сервером ідентифікації серверу прикладної системи відповіді з маркером доступу у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «access_token»:«»,
   «token_type»:«bearer»,
   «expires_in»:«»
}
```

Параметри відповіді описані у табл.3.1.

Таблиця 3.1 – Опис параметрів відповіді серверу прикладної системи з маркером доступу

Параметри	Опис
access_token	Маркер доступу (значення маркеру наведене для прикладу)
token_type	Тип маркеру доступу (має фіксоване значення для застосування засобами ідентифікації – **bearer** – доступ за маркером для пред'явника)
expires_in	Час завершення дії маркеру доступу

У сервері ідентифікації ідентифікатори ідентифікованих користувачів (**user_id**) зберігаються разом з інформацією з сертифікатів користувачів у тимчасовій базі даних (БД) і час завершення дії маркеру доступу (**expires_in**) вказує на термін існування відповідних записів у БД. У разі помилки обробки запиту відправляється структура у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «error»:«invalid_grant»,
   «error_description»:«»
}
```

3.2 Запит на видалення даних сесії користувача

Запит складається з таких кроків:

1. відправку сервером прикладної системи запита серверу ідентифікації на видалення даних сесії користувача за маркером доступу (**access_token**) методом GET чи POST протоколу HTTPS виду:

```
GET / POST
https://id.gov.ua/get-user-logout?access_token=&user_id=36
```

Параметри запиту описані у табл. 3.2.

Таблиця 3.2 – Опис параметрів запиту на отримання інформації про користувача сервером прикладної системи

Параметри	Опис
access_token	Маркер доступу
user_id	Ідентифікатор ідентифікованого користувача (значення наведене для прикладу)

2. обробку запиту та відправку сервером ідентифікації серверу прикладної системи відповіді з маркером доступу у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «error»:«0»,
   «error_description»:« Дані користувача із ID = user_id видалено успішно»
}
```

У разі помилки обробки запиту відправляється структура у вигляді JSON-тексту виду:

```
Content-Type: application/json
{
   «error»:«1»,
   «error_description»:«»
}
```

4 ПОРЯДОК ПІДКЛЮЧЕННЯ ВІДЖЕТУ ПІДПИСУ

Для підключення віджету до стороннього web-сайту необхідно:
1) внести DNS-ім'я web-сайту до переліку дозволених AllowedWebSites.lst (1);
2) за необхідності, створити окремі файли для зміни зовнішнього вигляду [DNS-ім'я web-сайту].css віджету (2) та налаштувань [DNS-ім'я web-сайту].json (3).

Для підключення віджету до сторінки web-сайту необхідно:
1) підключити скрипт взаємодії eusign.js до сторінки:
```
<script type="text/javascript" src="eusign.js"></script>
```
2) створити батківський елемент на сторінці в якому буде відображатися iframe:
```
<div id="sign-widget-parent" style="width:700px;height:500px">
```
3) створити об'єкт для взаємодії з iframe:
```
var euSign = new EndUser(
    "sign-widget-parent",          /* Ідентифікатор батківського елементу */
    "sign-widget",                 /* Ідентифікатор елементу iframe */
    "https://eu.iit.com.ua/sign-widget/v20190408/",
                                   /* URI для завантаження iframe */
    EndUser.FormType.SignFile      /* Тип форми iframe */
);
```

Детальний опис методів та параметрів знаходиться в java-скрипт-файлі eusign.js.

Примітка 1,2,3. Дані додаються за зверненням на адресу agency@e.gov.ua