

ДАТА СТВОРЕННЯ ДОКУМЕНТА: 8/03/2024

РЕМ-HEART SIGNATURE ПОСІБНИК КОРИСТУВАЧА CENCERT

ПУБЛІЧНИЙ ДОКУМЕНТ

СТВОРЕНИЙ ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O. 02-230
ВАРШАВА

UL. JUTRZENKI 116 | ТЕЛЕФОН: +48 22 570 57 10 | FAX: +48 22 570 57 15

WWW.ENIGMA.COM.PL

ДАТА СТВОРЕННЯ ДОКУМЕНТА: 5/03/2024

ТИП ДОКУМЕНТА: ПУБЛІЧНИЙ

©2018 ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O.

ВСІ ПРАВА ЗАХИЩЕНІ. ЖОДНА ЧАСТИНА ВМІСТУ ЦЬОГО ДОКУМЕНТА НЕ МОЖЕ БУТИ ВІДТВОРЕНА В БУДЬ-ЯКІЙ ФОРМІ АБО БУДЬ-ЯКИМИ ЗАСОБАМИ БЕЗ ДОЗВОЛУ ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O.

ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O.

JUTRZENKI 116

02-230 ВАРШАВА

ПОЛЬЩА

ТЕЛЕФОН: +48 22 570 57 10

FAX: +48 22 570 57 15

ВЕБ-САЙТ: WWW.ENIGMA.COM.PL

ЗМІСТ

1	ВВЕДЕННЯ	6
2	БЕЗПЕКА ПРОДУКЦІЇ	8
3	ВСТАНОВЛЕННЯ	9
3.1	ВСТАНОВЛЕННЯ ДЛЯ системи Windows	9
3.1.1	ВСТАНОВЛЕННЯ	9
3.1.2	Видалення програми	12
3.2	Встановлення для системи MacOS	13
3.2.1	Встановлення через файловий менеджер	15
3.2.2	Встановлення програми SafeNet Client	19
3.2.3	Видалення програми	24
3.2.4	Видалення SafeNet Client	25
3.3	Встановлення для системи Linux	27
3.3.1	Встановлення через файловий менеджер	28
3.3.2	Встановлення через командний рядок	29
3.3.3	Видалення програмного забезпечення	29
4	ФАЙЛОВІ ОПЕРАЦІЇ	31
4.1	Подача підписів – підпис на картці або USB-токені	31
4.2	Подача підписів – підпис rSign (хмарний підпис)	32
4.3	Перевірка підпису	33
4.3.1	Панель перевірки	35
5	ОСНОВНІ ФУНКЦІЇ	39
5.1	Запуск програми	39

5.2	Підпис у програмі	39
5.2.1	Подача підписів – підпис на картці або USB-токені	39
5.2.2	Надсилання підписів – підпис rSign (хмарний підпис).....	42
5.3	Перевірка підпису в програмі	46
6	РОЗШИРЕНІ ФУНКЦІЇ.....	49
6.1	Контрасигнатура	50
6.2	Позначення часу	51
6.3	Підписання XML-документа з вкладеннями	52
7	ПІДТРИМКА КРИПТОГРАФІЧНИХ КАРТ У ПРОГРАМІ	55
7.1	Зміна PIN-коду	55
7.2	Розблокування карти	58
7.3	Діагностика	60
7.4	Додаткові опції	61
7.4.1	Відновлення сертифіката.....	61
7.4.2	Конфігурація rSign.....	61
8	НАЛАШТУВАННЯ ПРОГРАМИ	62
8.1	Зміна параметрів підпису.....	62
8.2	Файли	64
8.3	Проксі	65
8.4	Pin	67
8.5	Сертифікати	67
8.6	TSL списки	69
8.7	Налаштування мови.....	70
8.8	Оновлення	70

8.9	Імпорт даних.....	71
8.9.1	Очищення кешу.....	72
9	ПІДПИС RSIGN	73
9.1	Конфігурація на комп'ютері	73
9.1.1	Додавання токена rSign	73
9.1.2	Видалення токена rSign.....	75
9.2	Налаштування мобільного додатку.....	76
9.2.1	Встановлення	76
9.2.2	Домашній екран	76
9.2.3	Ідентифікатор ключа	77
9.2.4	Налаштування	78
10	АДМІНІСТРУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ REM-HEART	80
10.1	Журнали роботи карток для систем Windows	80
11	ВИРІШЕННЯ ПРОБЛЕМ.....	84
12	СПИСОК МАЛЮНКІВ.....	86

1 ВВЕДЕННЯ

Програмне забезпечення PEM-HEART Signature використовується для:

- подання кваліфікованих підписів або електронних печаток на основі сертифікатів, виданих Cencert,
- перевірка кваліфікованих електронних підписів (у тому числі підписів на основі сертифікатів, виданих в інших країнах ЄС), протягом терміну дії сертифіката.

Додатково:

- перевірка електронних підписів після закінчення терміну дії сертифіката, якщо підпис знаходиться в архівній формі (див. опис архівної форми в гл. [4.3.1 Панель перевірки](#)),
- перевірка підписів на основі звичайних (некваліфікованих) сертифікатів, виданих Cencert.

PEM-HEART Signature створює електронні підписи у форматах:

- XAdES відповідно до технічних умов ETSI TS 101 903 XML Advanced Electronic Signatures (XadES),
- CAdES CMS відповідно до технічних умов ETSI TS 101 733 Electronic Signature Format (CAdES to skrót od CMS Advanced Electronic Signatures),
- PAdES (стандарт ETSI TS 102 778) - PDF Advanced Electronic Signatures,
- ASiC (стандарт ETSI TS 102 918) - програма створює підпис у базовій формі ASX, створюючи файл із розширенням .asics . (файл містить базовий контейнер ASiC XadES навколо нього).

Ці формати визначають структуру файлу, що містить підпис. Для вибору певного формату потрібне програмне забезпечення, яке зможе перевірити правильність такого підпису.

Виробником рішень для Cencert є ENIGMA Systemy Ochrony Informacji Sp. z o.

Основним напрямком діяльності ENIGMA є розробка, виробництво та впровадження інноваційних систем захисту інформації. Використовуючи власні

апаратно-програмні рішення, забезпечує найкращий захист даних в органах державної влади та місцевого самоврядування, фінансових установах та підприємствах. Усі продукти ENIGMA забезпечують повний криптографічний захист зібраної, обробленої та переданої інформації. Пропоновані рішення сертифіковані на безпеку спеціалізованими підрозділами Держохорони.

Cencert є зареєстрованою торговою маркою ENIGMA Systemy Ochrony Informacji.

Cencert є кваліфікованою організацією, що надає кваліфіковані та некваліфіковані довірчі послуги з 2009 року – у сфері видачі сертифікатів, кваліфікованих часових позначок та послуги підтвердження дійсності сертифікатів (OCSP). Правовою основою для надання послуг Cencert є, зокрема, eIDAS (Регламент Європейського Парламенту та Ради (ЄС) № 910/2014), а також Закон про довірчі послуги та електронну ідентифікацію (Journal of Laws 2016 р., п. 1579).

2 БЕЗПЕКА ПРОДУКЦІЇ

Програма повинна використовуватися на комп'ютері, який знаходиться під контролем власника сертифіката. Комп'ютер має бути захищений від доступу неавторизованих осіб, мати встановлене найновіше антивірусне програмне забезпечення та актуальні оновлення операційної системи.

Електронні підписи не можна створювати на комп'ютерах, безпека яких невідома (наприклад, комп'ютери, доступні для громадськості чи широкого кола людей, комп'ютери випадкових людей тощо).

Програму слід використовувати в середовищі, де програмний код захищений від змін операційною системою. Цього можна досягти за допомогою операційних систем, які пропонують контроль доступу (Windows, Linux і MacOSX), або шляхом встановлення прав доступу до каталогів із виконуваними файлами так, щоб користувач не мав права змінювати виконувані файли, що містяться в них.

Програму слід використовувати в середовищі, в якому операційна система захищає від можливості перехоплення ворожими системами даних, що надсилаються через порти комп'ютера, а також даних, що вводяться з клавіатури комп'ютера у вікна програми. Цього можна досягти, використовуючи операційні системи, які пропонують контроль доступу (Windows, Linux і MacOSX) і забезпечуючи належний рівень захисту комп'ютера від авторизованих користувачів (захист шляхом встановлення відповідних прав доступу та постійного оновлення операційної системи), неавторизованих користувачів та атаки з комп'ютерної мережі (захист шляхом постійного оновлення операційної системи та, за необхідності, з використанням пристроїв firewall).

Програма, яка працює як «безпечний пристрій для створення та перевірки безпечних електронних підписів», не може використовуватися в «публічному середовищі», тобто в середовищі, в якому будь-яка фізична особа може мати доступ до програмного забезпечення за звичайних умов роботи.

Технічний компонент або додані до нього драйвери, які, окрім програми, є частиною «захищеного пристрою для створення та перевірки захищених електронних підписів», мають функцію знищення даних, які використовуються для створення підписів (тобто закритого ключа) на запит користувача. Знищення здійснюється в такому обсязі, щоб запобігти реконструкції цих даних на основі аналізу записів у пристроях, у яких вони були створені, збережені або використані.

3 ВСТАНОВЛЕННЯ

Інсталяційні пакети доступні на веб-сайті www.Cencert.pl:

<https://www.cencert.pl/do-pobrania/oprogramowanie-do-podpisu/>

3.1 ВСТАНОВЛЕННЯ ДЛЯ СИСТЕМИ WINDOWS

3.1.1 ВСТАНОВЛЕННЯ

Встановлення необхідно виконувати з облікового запису з правами адміністратора. Перед початком інсталяції рекомендується завершити роботу всіх програм, крім тих, які необхідні для роботи операційної системи.

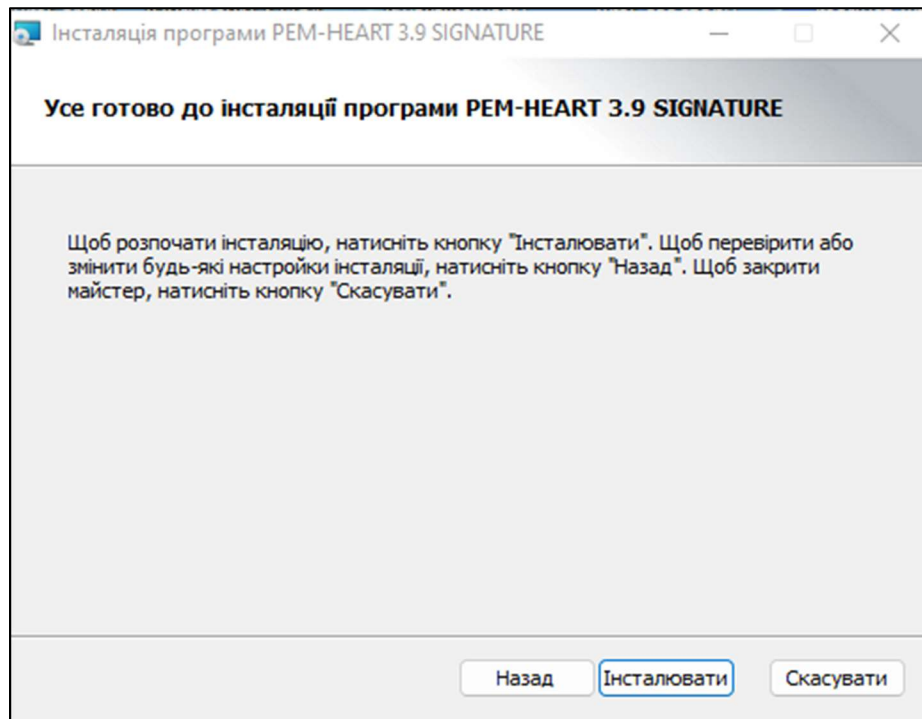
Процедура встановлення нижче представлена на прикладі системи Windows 11:

1. Запустіть інсталятор pemheart-signature.exe, який відобразить вікно початкової інсталяції.



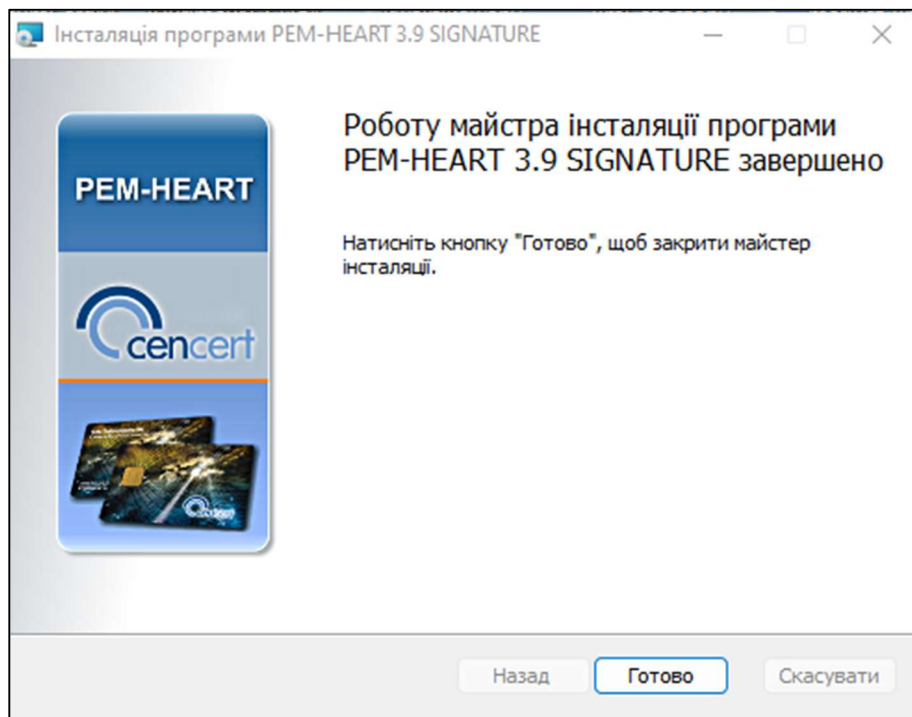
Мал. 1 Вікно запуску майстра встановлення

2. Натиснувши кнопку *Встановити*, буде запущено майстер встановлення продукту.



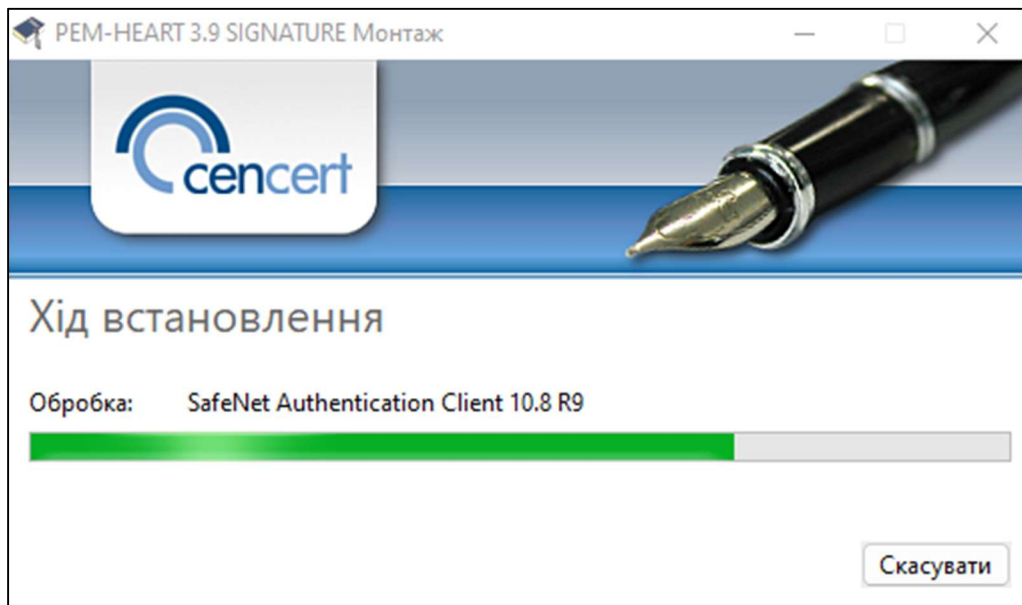
Мал. 2 Вікно майстра встановлення

3. Натисніть *Встановити*, почнеться встановлення програмного забезпечення.
4. Натисніть *Готово* — майстер завершить роботу. Це також запустить процес встановлення програмного забезпечення Thales SafeNet.



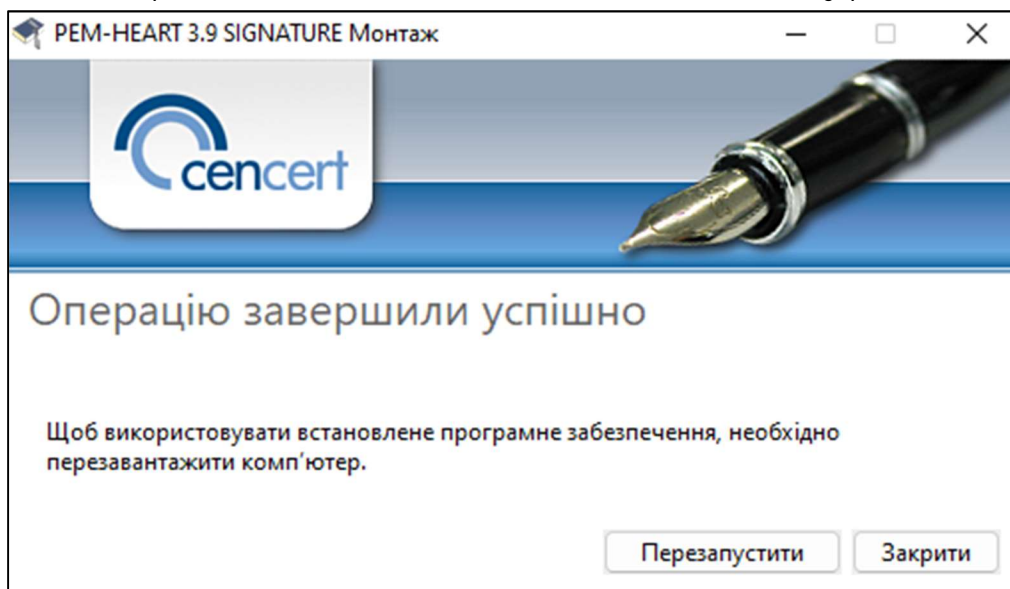
Мал. 3 Вікно, що завершує роботу майстра встановлення

5. З'явиться майстер встановлення програмного забезпечення Thales SafeNet.



Мал. 4 Встановлення Thales SafeNet

6. Натисніть *Перезавантажити* - це необхідно для початку роботи з програмою.

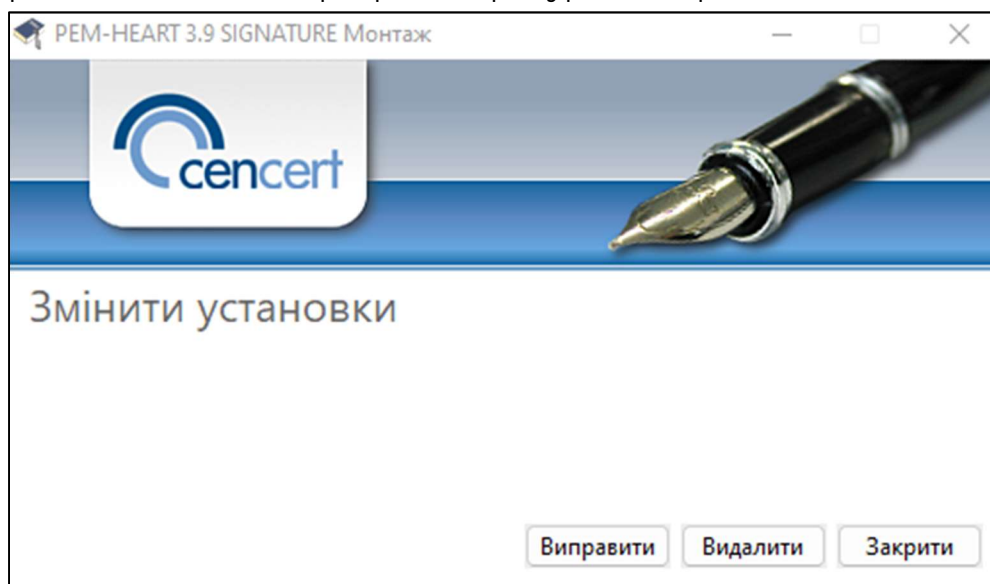


Мал. 5 Вікно для завершення процесу встановлення

3.1.2 ВИДАЛЕННЯ ПРОГРАМИ

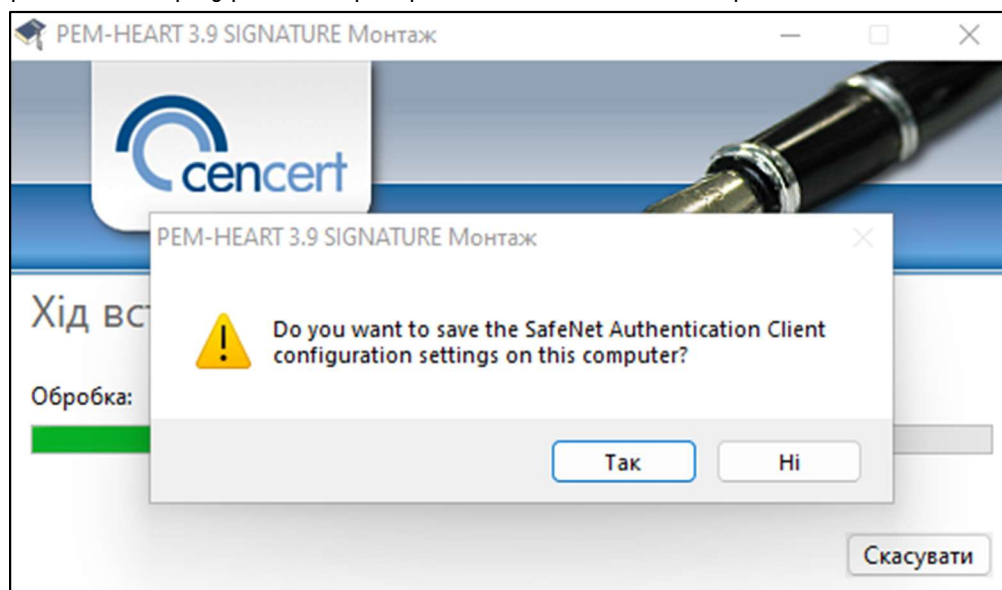
Програму можна видалити, вибравши пакет «PEM-HEART SIGNATURE» на панелі керування Windows: Панель керування\Програми\Програми та функції.

1. Запуститься майстер встановлення. Натисніть кнопку Видалити - програма почне процес видалення програми з ресурсів операційної системи.



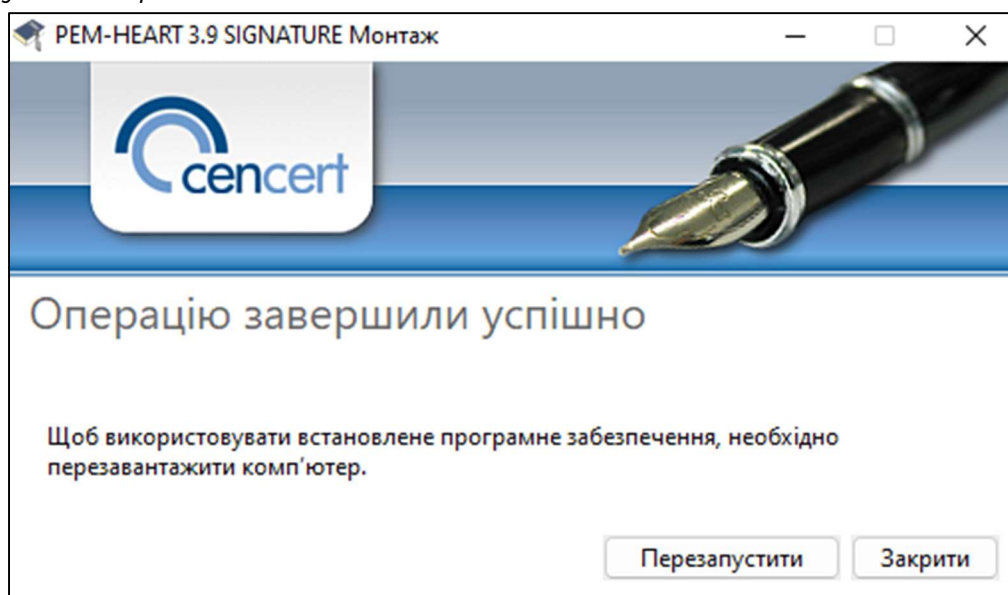
Мал. 6 Можливості модифікації встановлення

2. Під час процесу буде відображено повідомлення з проханням видалити або зберегти конфігурацію програми SafeNet для карток Thales.



Мал. 7 Видалення програми

3. 3. Майстер встановлення повідомить вам, що процес видалення програмного забезпечення завершено. Вам потрібно перезавантажити комп'ютер, натиснувши *Перезавантажити*.



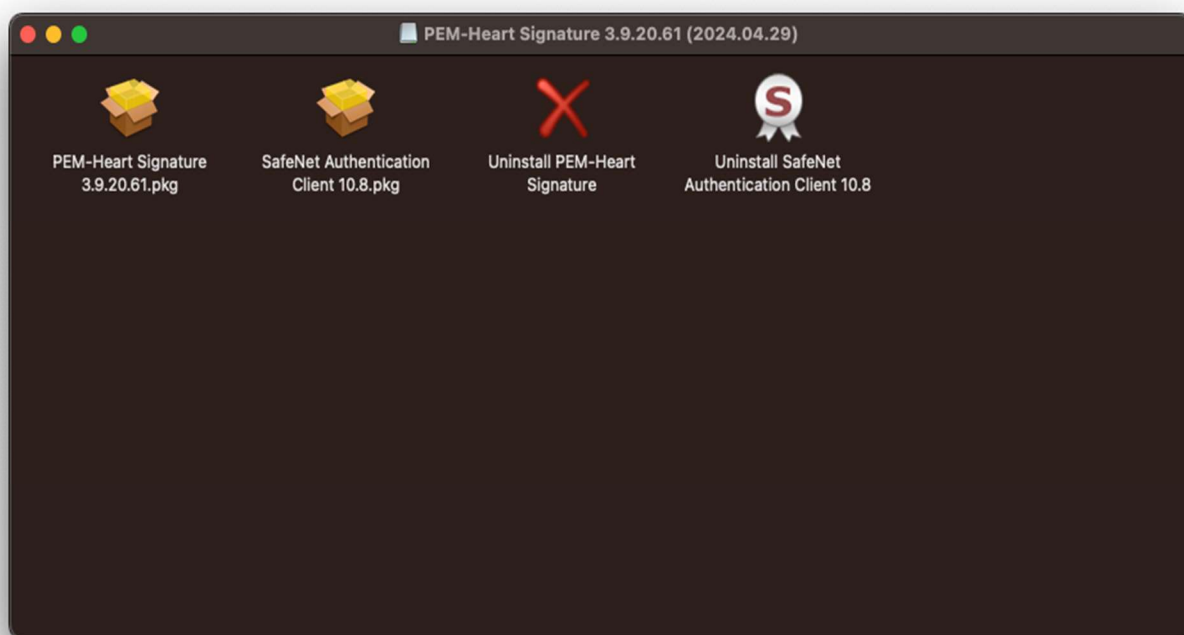
Мал. 8 Підтвердження видалення програми

3.2 ВСТАНОВЛЕННЯ ДЛЯ СИСТЕМИ MACOS

Пакет Pem-Heart для MacOS поширюється у форматі .dmg - він містить файли встановлення та програми видалення.

Pem-Heart підтримує macOS версії 13 (Ventura) і 14 (Sonoma).

Наведені нижче інструкції базуються на MacOS Ventura.



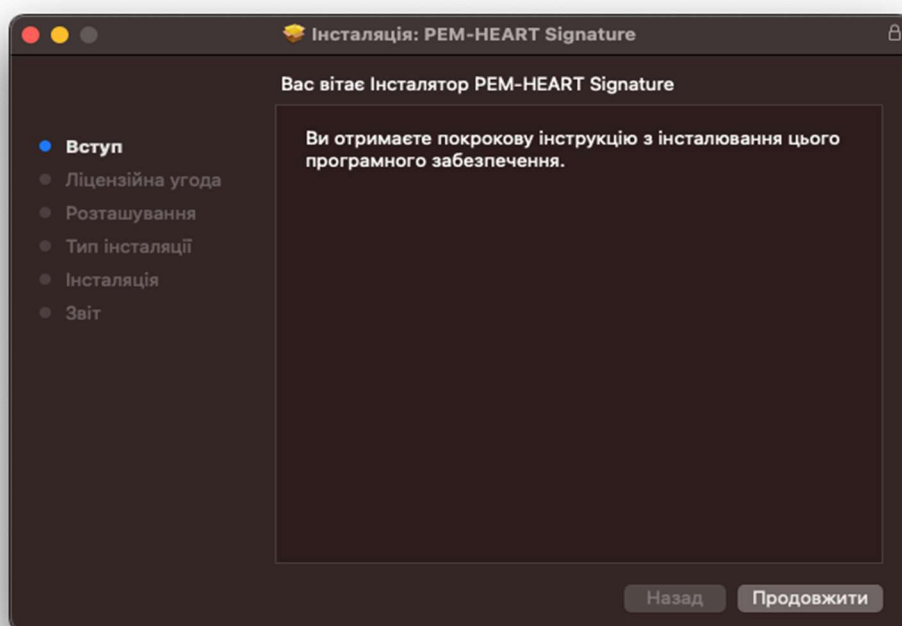
Мал. 9 Пакет PemHeart для macOS

3.2.1 ВСТАНОВЛЕННЯ ЧЕРЕЗ ФАЙЛОВИЙ МЕНЕДЖЕР

Встановлення необхідно виконувати з облікового запису з правами адміністратора. Перед початком інсталяції рекомендується завершити роботу всіх програм, окрім тих, які необхідні для роботи операційної системи.

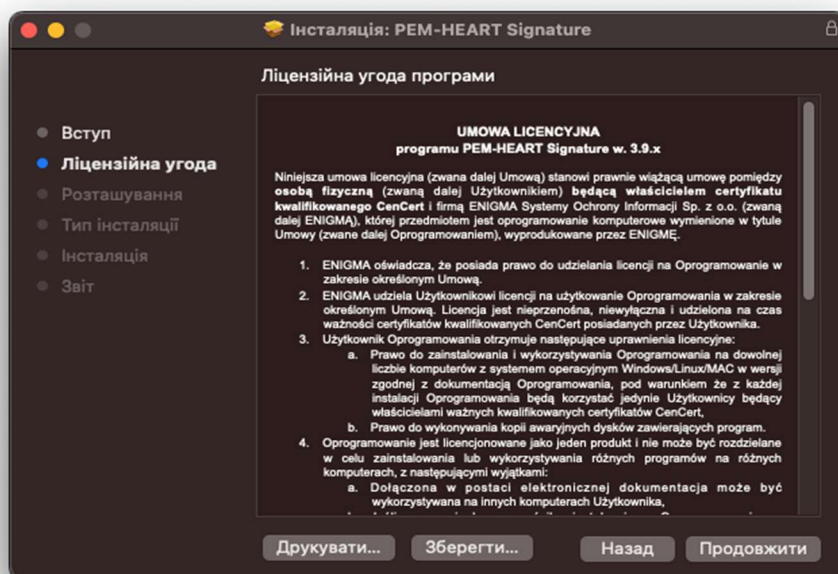
Доступні версії програми для процесорної архітектури INTEL і ARM

У файловому менеджері Finder знайдіть місце з інсталяційним файлом PEM-HEART Signature у файловій структурі. Запустіть файл, це ініціалізує програму встановлення.

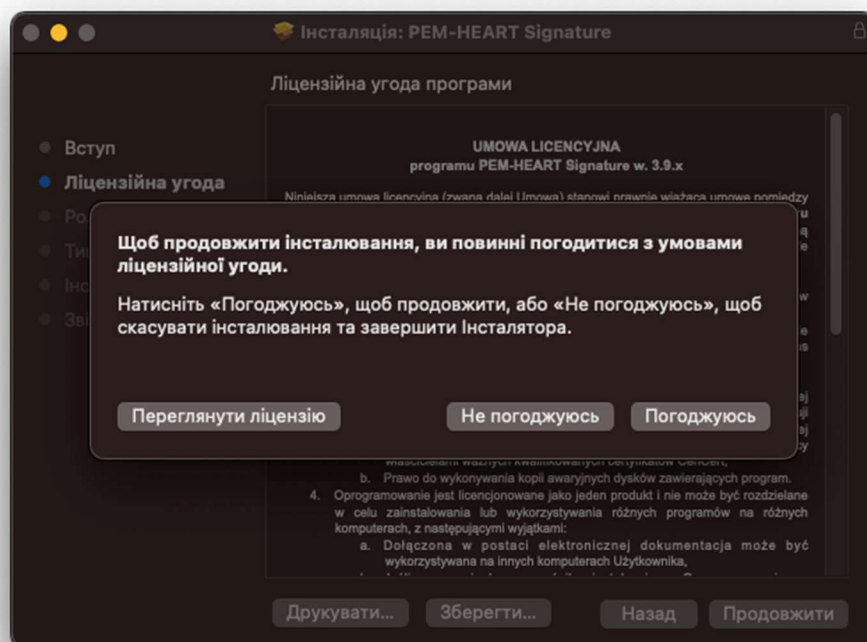


Мал. 10 Встановлювач пакетів Pem-Heart - вікно запуску

1. На першому етапі інсталяції користувач повинен прийняти ліцензійну угоду.

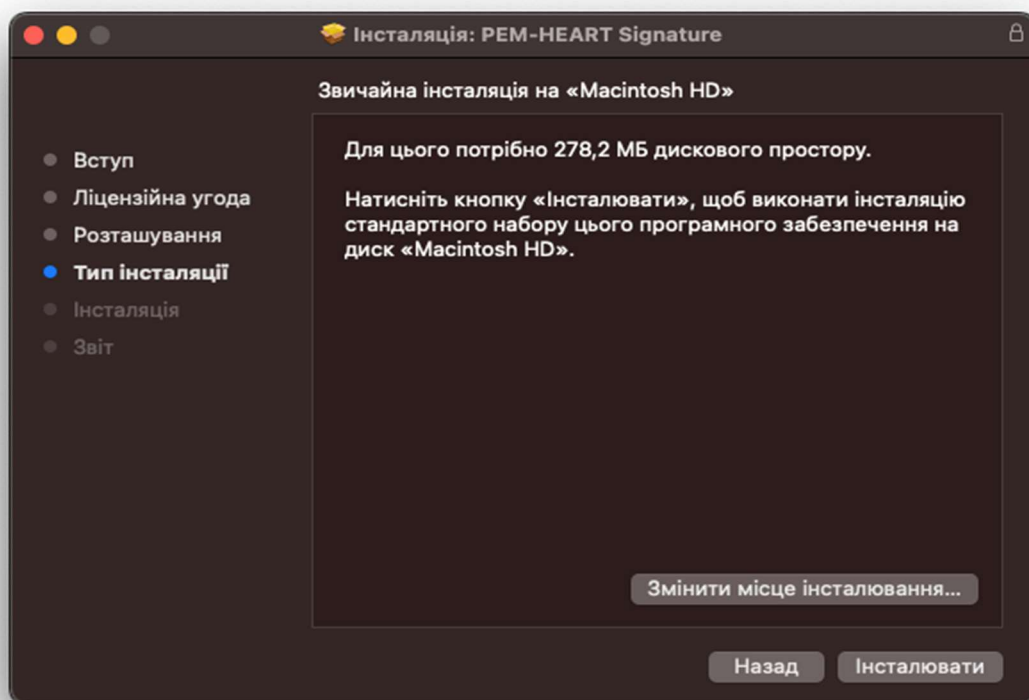


Мал. 11 Встановлювач пакетів Pem-Heart - ліцензійна угода



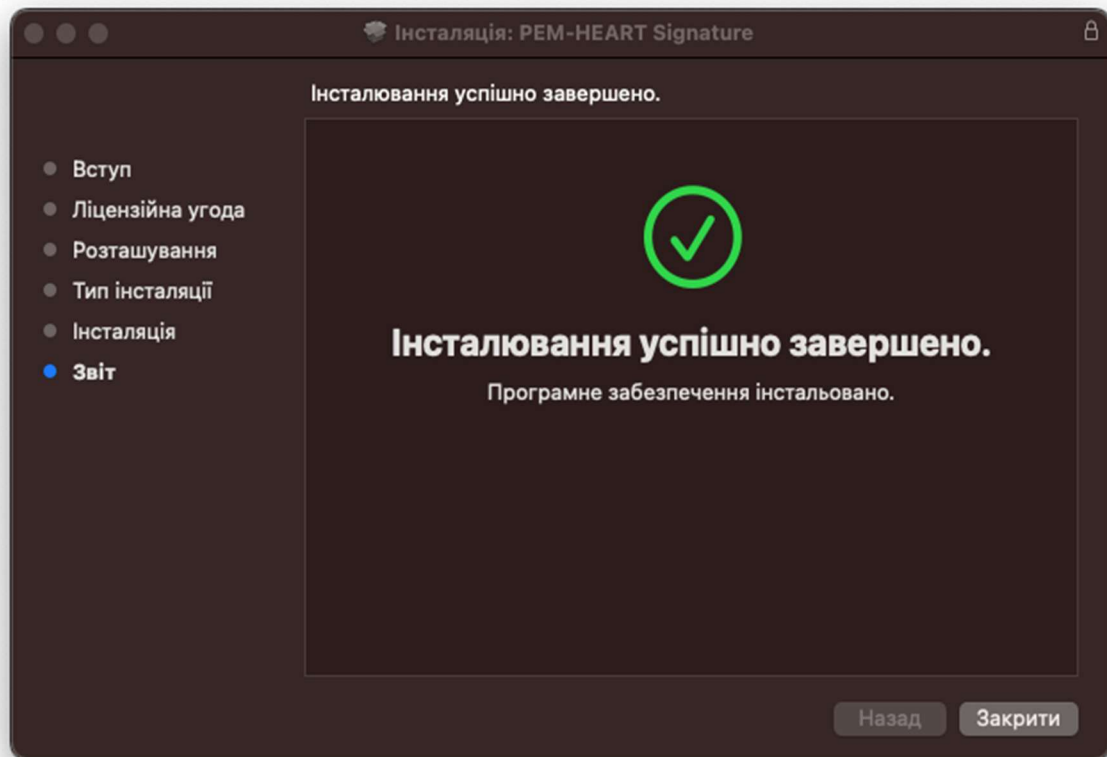
Мал. 12 Встановлювач пакетів Pem-Heart - прийняття ліцензійної угоди

2. Потім підтвердіть свій намір інсталювати, натиснувши кнопку *Встановити* та ввівши пароль облікового запису користувача — почнеться процес інсталяції. На цьому етапі також можна змінити місце встановлення, натиснувши *Змінити місце встановлення...* .



Мал. 13 Встановлювач пакетів Pem-Heart - інформація про встановлення

3. Після завершення процесу інсталяції відобразиться екран із підсумками.



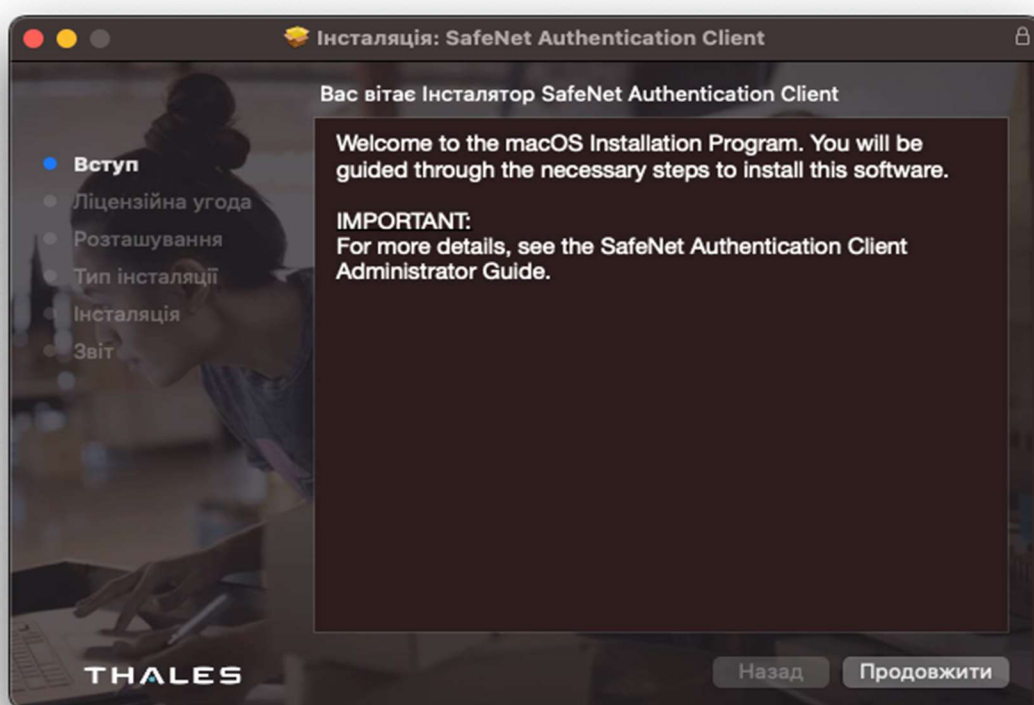
Мал. 14 Встановлювач пакетів Pem-Heart - підсумок встановлення

3.2.2 ВСТАНОВЛЕННЯ ПРОГРАМИ SAFENET CLIENT

Програма Thales SafeNet підтримує карти IDPrime.

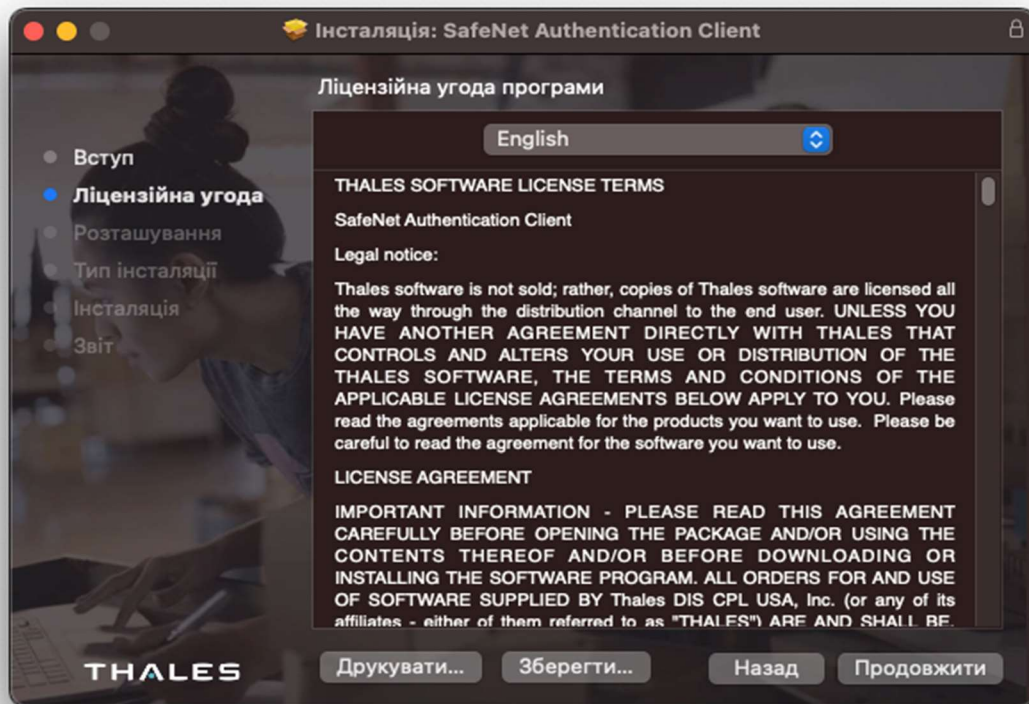
Встановлення необхідно виконувати з облікового запису з правами адміністратора. Перед початком інсталяції рекомендується завершити роботу всіх програм, окрім тих, які необхідні для роботи операційної системи.

У файловому менеджері Finder знайдіть інсталяційний файл SafeNet Authentication Client у файловій структурі. Запуск файлу ініціалізує програму встановлення.

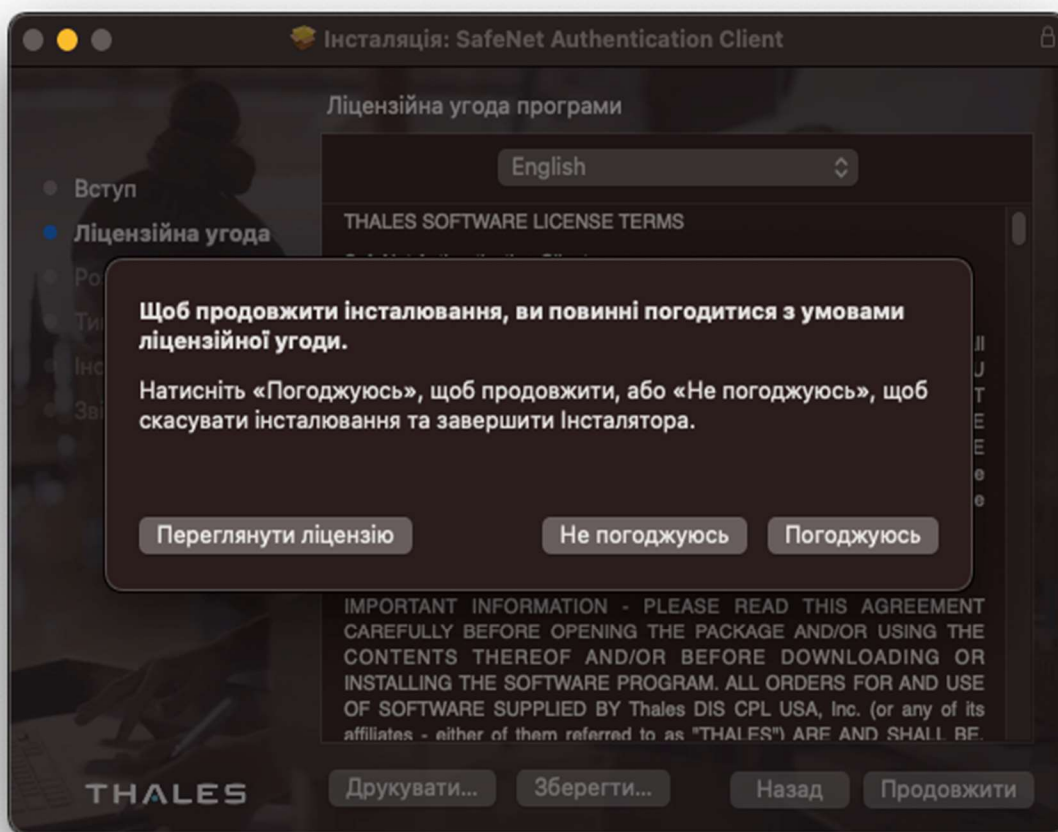


Мал. 15 Встановлювач пакетів SafeNet Authentication Client - вікно запуску

1. На першому етапі інсталяції користувач повинен прийняти ліцензійну угоду.

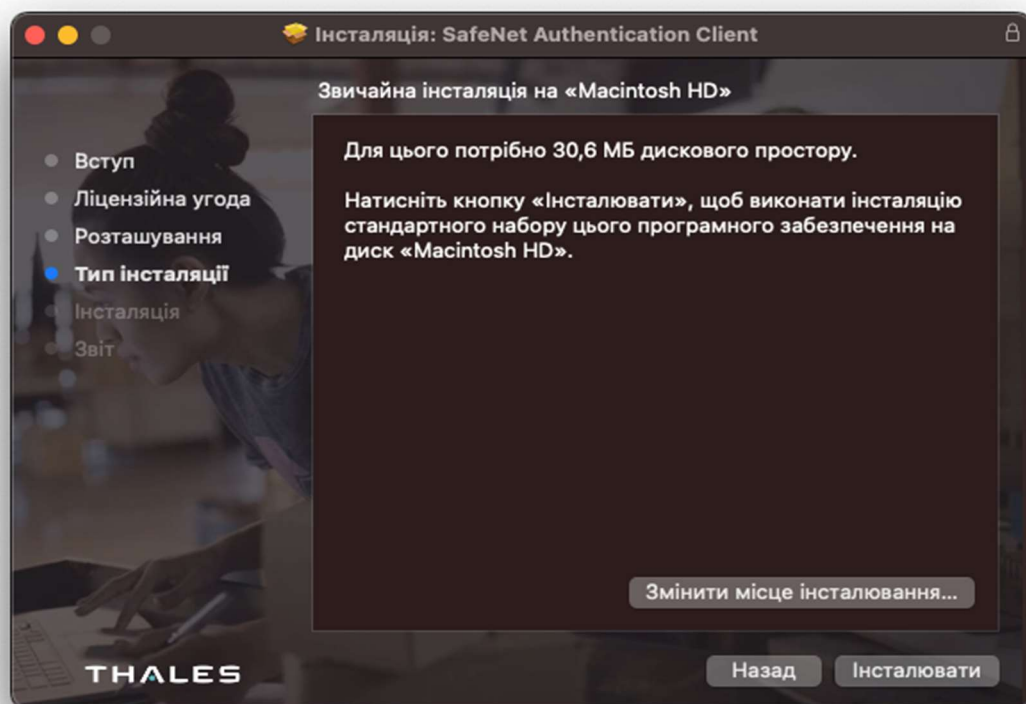


Мал. 16 Встановлювач пакетів SafeNet Authentication Client – ліцензійна угода



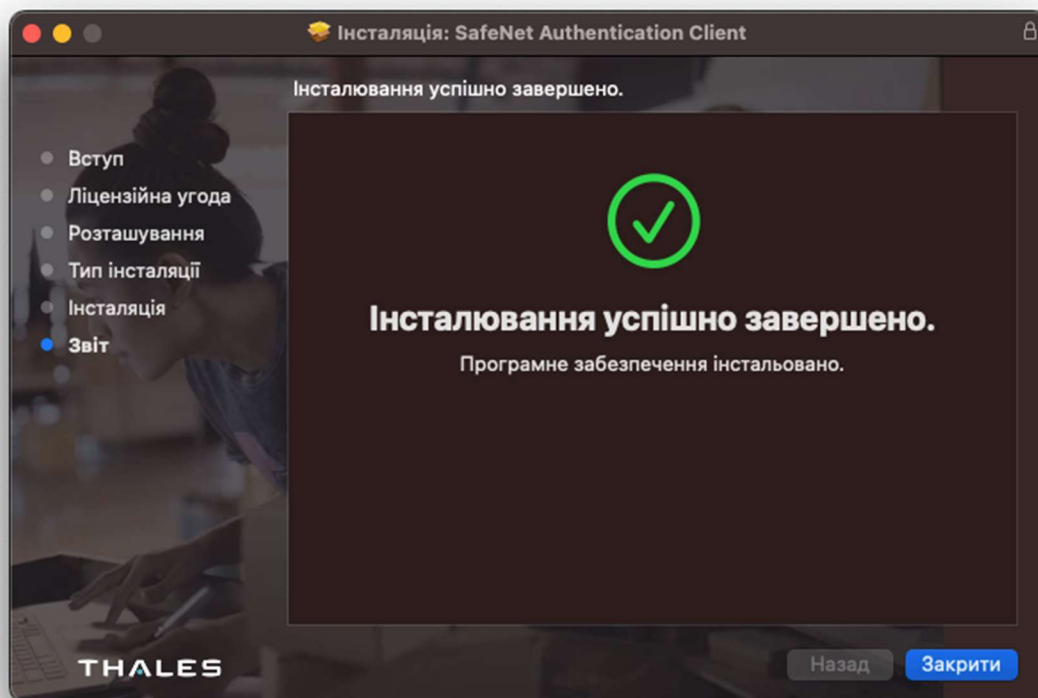
Мал. 17 Встановлювач пакетів SafeNet Authentication Client - прийняття ліцензійної угоди

- Потім підтвердіть свій намір інсталювати, натиснувши кнопку *Встановити* та ввівши пароль облікового запису користувача — почнеться процес інсталяції. На цьому етапі також можна змінити місце встановлення, натиснувши «Змінити місце встановлення...».



Мал. 18 Встановлювач пакетів SafeNet Authentication Client – інформація про встановлення

- Після завершення процесу інсталяції відобразиться екран із підсумками.

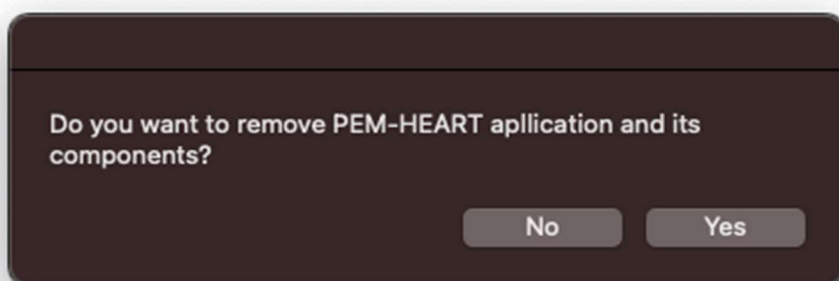


Мал. 19 Встановлювач пакетів SafeNet Authentication Client - підсумок встановлення

3.2.3 ВИДАЛЕННЯ ПРОГРАМИ

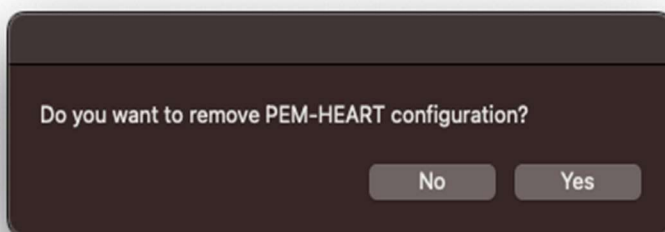
Видалення виконується після запуску програми *Uninstall PEM-Heart Signature*. З'являться діалогові вікна із запитом про згоду на видалення:

- Додаток PEM-HEART разом з окремими програмними компонентами,



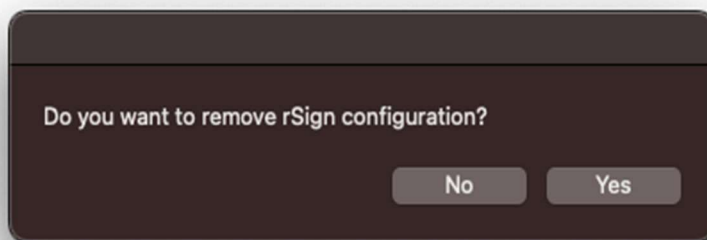
Мал. 20 Повідомлення про видалення додатку Pem-Heart із запитом на видалення

- конфігурації PEM-HEART з каталогів opt, etc і home,



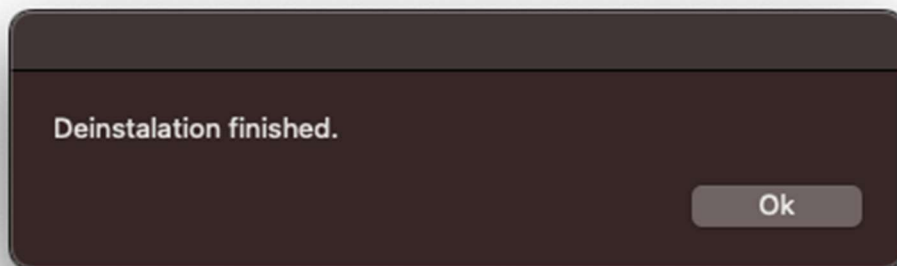
Мал. 21 Повідомлення про видалення із запитом на видалення конфігурації Pem-Heart

- Конфігураційні файли rSign (enigmaCloud.ini).



Мал. 22 Повідомлення про видалення із запитом на видалення конфігурації rSign

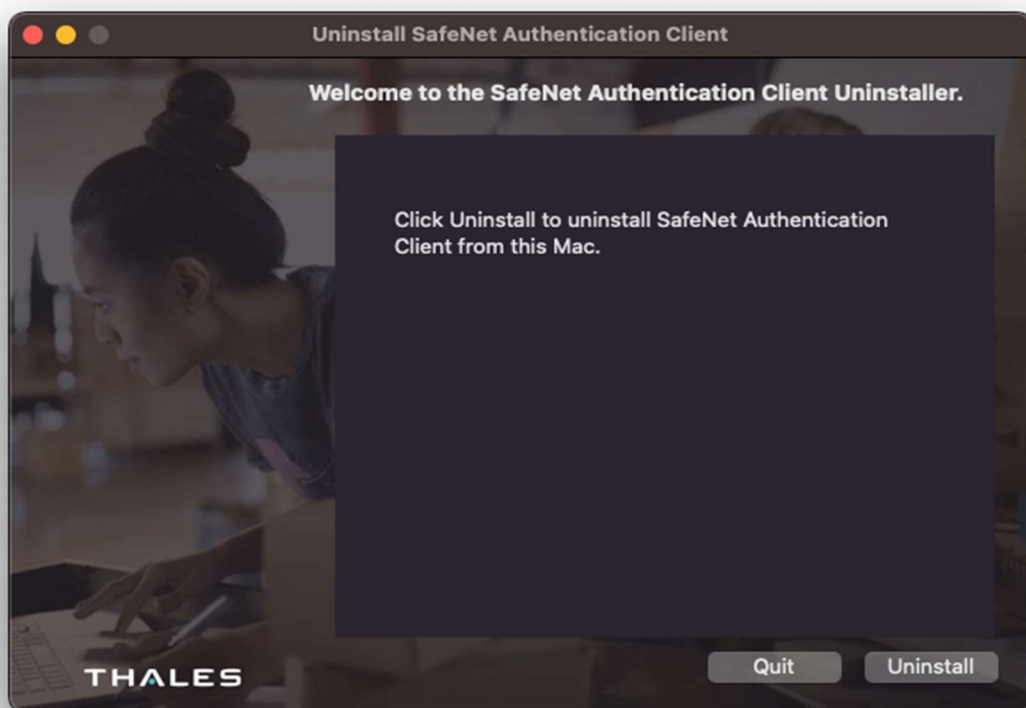
Після завершення процесу з'явиться вікно з підтвердженням видалення:



Мал. 23 Підтвердження видалення програми

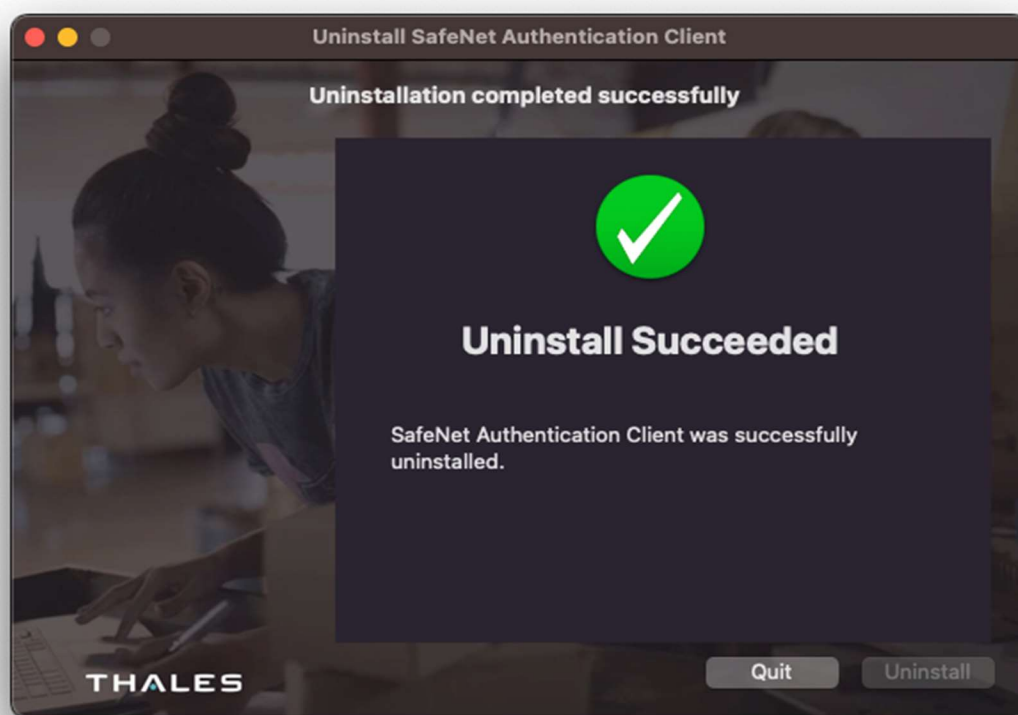
3.2.4 ВИДАЛЕННЯ SAFENET CLIENT

Видалення програмного забезпечення для керування картками Thales здійснюється з панелі керування, у опції *Програми та засоби*, де потрібно вибрати програму зі списку доступних і вибрати опцію *Видалити* або *Видалити/змінити*.



Мал. 24 Програма видалення SafeNet Authentication Client – вікно запуску

У вікні майстра видалення натисніть Видалити та введіть свій пароль. Буде відображено підтвердження процесу.



Мал. 25 Програма видалення SafeNet Authentication Client – підсумок видалення

3.3 ВСТАНОВЛЕННЯ ДЛЯ СИСТЕМИ LINUX

Встановлення необхідно виконувати з облікового запису з правами адміністратора. Перед початком інсталяції рекомендується завершити роботу всіх програм, крім тих, які необхідні для роботи операційної системи.

Наступна процедура встановлення представлена на прикладі системи Ubuntu 20.04 LTS у системному менеджері пакетів (наприклад, Ubuntu Software) і через термінал із командного рядка.

Операції інсталяції пакета має передувати інсталяція необхідних пакетів: `pcscd` і `libncurses5`. Це можна зробити за допомогою команд:

```
sudo apt-get install pcscd
```

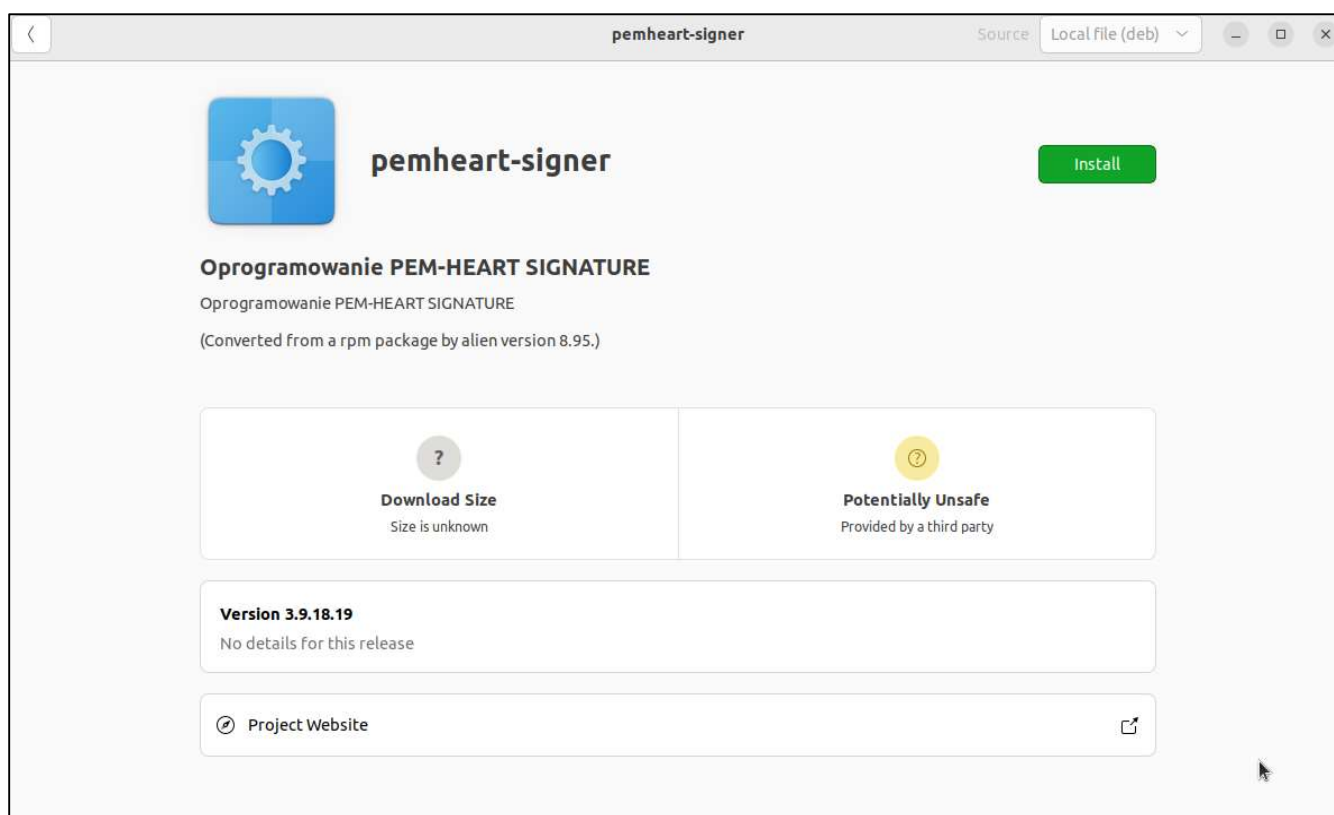
```
sudo apt-get install libncurses5
```

3.3.1 ВСТАНОВЛЕННЯ ЧЕРЕЗ ФАЙЛОВИЙ МЕНЕДЖЕР

У менеджері знайдіть у файловій структурі місце, де розташовані файли встановлення PEM-HEART Signature. Встановлення виконується шляхом запуску (подвійного клацання) заданого файлу. Потім відкриється стандартний пов'язаний менеджер пакетів. Після натискання кнопки *Встановити* PEM-HEART Signature встановлюється в систему.

Після завершення інсталяції з'явиться відповідне повідомлення, і вікно інсталятора можна буде закрити. На завершення встановіть програму Safenet Authentication Client, щоб увімкнути використання всіх доступних карток. Інсталяційний файл можна завантажити з веб-сайту cencert.pl.

Safenet Authentication Client під час інсталяції потрібен пакет libgdk-pixbuf2.0-0, встановлений у системі. Після встановлення доступ до програми можливий через контекстне меню файлів або через системне меню програм.



Мал. 26 Встановлення програми для Linux через файловий менеджер

Для встановлення натисніть зелену кнопку у верхньому правому куті *Install*.

3.3.2 ВСТАНОВЛЕННЯ ЧЕРЕЗ КОМАНДНИЙ РЯДОК

Варіант встановлення PEM-HEART Signature за допомогою командного рядка показаний нижче.

Після запуску вікна терміналу знайдіть у файловій структурі місце, де розташовано інсталяційні файли. Програмне забезпечення поширюється у вигляді інсталяційного пакета (файл із розширенням .deb). Щоб установити пакет «PEM-HEART Signature» на Ubuntu (тут у версії 20.4 LTS), виконайте команду:

```
sudo dpkg -i PH-3.9.X.X_amd64.deb
```

де X.X - номер випущеної версії програмного забезпечення.

3.3.3 ВИДАЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Щоб видалити програмне забезпечення із системи, ви можете скористатися терміналом із командним рядком або запустити менеджер пакетів.

- Видалення за допомогою командного рядка

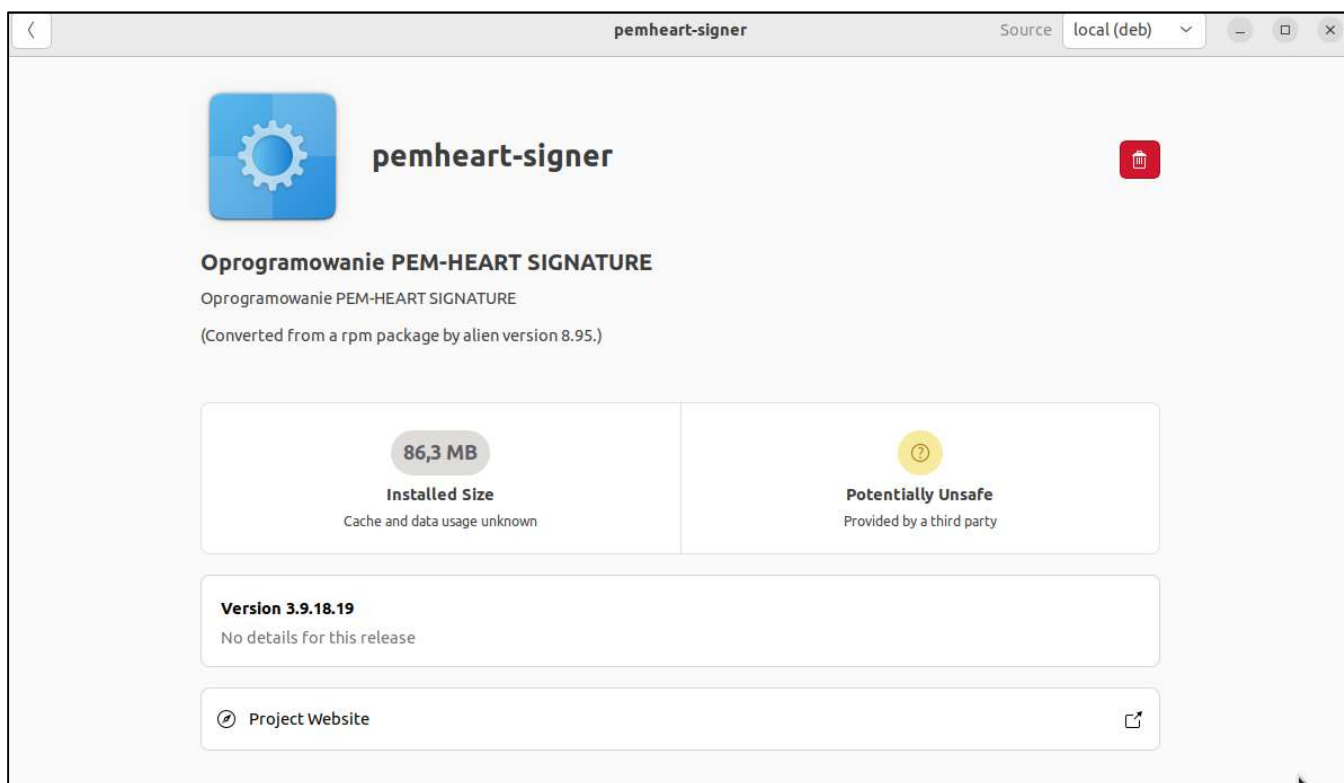
Видалення PEM-HEART Signature виконується за допомогою двох консольних програм:

```
sudo apt-get purge pemheart-signer або
```

```
sudo apt remove pemheart-signer
```

- Видалити за допомогою файлового менеджера

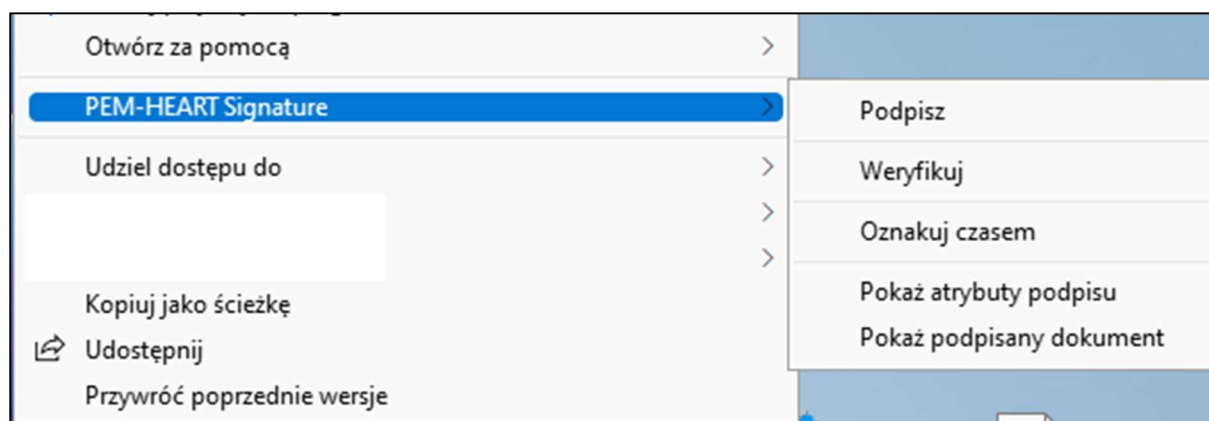
Після запуску менеджера пакунків (у прикладі використовувалося програмне забезпечення Ubuntu), знайдіть pemheart-signer на вкладці «Встановлено», а потім клацніть червоний смітник ([Мал. 27 Програма видалення програми для Linux через файловий менеджер](#)).



Мал. 27 Програма видалення програми для Linux через файловий менеджер

4 ФАЙЛОВІ ОПЕРАЦІЇ

Користувач може виконати деякі операції без безпосереднього запуску програми - клацнувши правою кнопкою миші (PPM) на файлі. З контекстного меню доступні різні функції, зокрема: проставлення підпису або завірення підпису. Залежно від типу файлу вибір параметрів може відрізнятися.



Мал. 28 Приклад функцій PPM для файлу PDF

4.1 ПОДАЧА ПІДПИСІВ – ПІДПИС НА КАРТЦІ АБО USB-ТОКЕНІ

Щоб підписати, вставте картку Cencert (токен у USB-порт USB-зчитувача), потім клацніть правою кнопкою миші (PPM) на файлі, який потрібно підписати, щоб розгорнути контекстне меню - виберіть наступні параметри *PEM-HEART Signature* -> *Підписати* (для багатьох програм ця опція може бути під Показати додаткові параметри). Операція також виконується з рівня запущеної програми PEM-HEART Signature (опис діяльності представлено [5.2.1 подача підписів – підпис на картці або USB-токені](#))

Програма автоматично вибере рекомендований формат підпису та запитає PIN-код картки.

Коментарі:

- Додаткові параметри, такі як зміна формату підпису, підпис в окремому файлі, відмітка часу та інші налаштування доступні під кнопкою *Параметри...* Налаштування, змінені таким чином, застосовуються до конкретного підпису

та не запам'ятовуються для подальшого використання. Дивіться також розділ **8.1 Зміна параметрів підпису**.

- Залежно від формату підпису, він буде збережено в тому самому файлі без зміни назви або в новому файлі зі зміненим розширенням.
- Якщо вибрати «підпис в окремому файлі», то підпис буде збережено в окремому файлі. Вибір цього параметра вимагає згодом надіслати одержувачу два файли: вихідний файл і підпис.
- Якщо підпис має містити мітку часу та/або відповідь OCSP, під час підпису потрібне підключення до Інтернету. Вам також може знадобитися придбати послугу штампування часу.

4.2 ПОДАЧА ПІДПИСІВ – ПІДПИС RSign (ХМАРНИЙ ПІДПИС)

Щоб підписати, клацніть правою кнопкою миші (PPM) файл, який потрібно підписати, щоб розгорнути контекстне меню - вибрати наступні параметри: *PEM-HEART Signature -> Підписати* (для багатьох додатків опція може бути під *Показати додаткові параметри*). Операція також виконується з рівня запущеної програми PEM-HEART Signature (подано опис діяльності у **5.2.2 Надсилання підписів – підпис rSign (хмарний підпис)**)

Програма автоматично вибере рекомендований формат підпису. Потім натисніть Далі та введіть свій PIN-код для підпису (користувачу буде запропоновано його ввести). Наступним кроком необхідно запустити на мобільному пристрої додаток rSign by Cencert, з якого з екрану потрібно зчитати код *АКТИВНИЙ ПІН ПІДПISУ* — ввести його в додаток на комп'ютері та натиснути ОК. Далі необхідно підтвердити свій намір підписати в додатку rSign, після чого програма виконає підпис.

Увага! Ми рекомендуємо встановити в додатку опцію *Налаштування -> PIN -> Запам'ятати PIN* на певний період часу, встановивши час 3 хвилини. Це дозволить вам поставити підпис із міткою часу або навіть кілька підписів (якщо програма вказала багато файлів для підпису) без необхідності затвердження кожної операції підпису на телефоні. Якщо для підпису встановлено значення «Запитувати PIN-код щоразу», створення підпису з міткою часу потребуватиме подвійного підтвердження підпису на телефоні (підпис під документом, підпис під запитом на мітку часу).

Увага:

- Додаткові параметри, такі як зміна формату підпису, підпис в окремому файлі, відмітка часу та інші налаштування доступні під кнопкою *Параметри...* Налаштування, змінені таким чином, застосовуються до конкретного підпису та не запам'ятовуються для подальшого використання. Дивіться також розділ **8.1 Зміна параметрів підпису**.
- Залежно від формату підпису, підпис буде збережено в тому ж файлі без зміни назви або в новому файлі зі зміненим розширенням.
- Якщо вибрати «підпис в окремому файлі», то підпис буде збережено в окремому файлі. Вибір цього параметра вимагає згодом надіслати одержувачу два файли: вихідний файл і підпис.
- Для підписання потрібне підключення до Інтернету.

4.3 ПЕРЕВІРКА ПІДПISУ

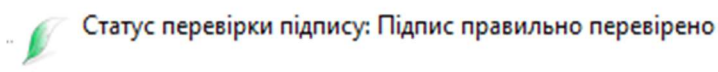
Щоб перевірити підпис, клацніть правою кнопкою миші (ПКМ) на файлі, який потрібно підписати, а потім виберіть команду *PEM-HEART Signature -> Перевірте* (для багатьох програм цей параметр може бути під *Показати додаткові параметри*). Після цього відобразиться вікно перевірки підпису. Потім натисніть кнопку *Перевірити*. Програма перевірить підписи, збережені в документі, і відобразить результат перевірки. Операція також виконується з запущеної програми PEM-HEART Signature (опис дій представлено в **5.3 Перевірка підпису в програмі**)

Якщо підпис був позначений міткою часу - момент, для якого перевіряється підпис, береться з мітки часу (будь-яке подальше відкликання сертифіката не вплине на результат перевірки такого підпису).

Якщо підпис не має позначки часу - підпис перевіряється в поточний момент або в інший момент, введений вручну в програму («перевірити за вказаний час: ...»). Якщо ви вручну вводите момент, для якого перевіряється підпис, то відповідальність за правильність часу (і, можливо, доказовість) повністю лежить на користувачеві.

Результат перевірки позначається кольоровими символами для чіткого розрізнення:

- Зелений колір означає правильну перевірку підпису.



- Жовтий колір означає неповну перевірку – підпис математично правильний, але поки що неможливо підтвердити, чи був сертифікат дійсним на момент підписання. У цьому випадку вам слід повторити перевірку пізніше - наприклад, через кілька годин або наступного дня.



Статус перевірки підпису: Підпис не повністю перевірено. Термін дії сертифіката користувача закінчився. Список CRL відсутній для повної перевірки виданий до закінчення терміну дії сертифіката.

- Червоний колір означає неможливість перевірки підпису (наприклад, математична невідповідність, тобто порушення цілісності документа або твердження про те, що сертифікат недійсний).



Статус перевірки підпису: Підпис не піддається перевірці. Немає можливості створити шлях сертифікації

4.3.1 ПАНЕЛЬ ПЕРЕВІРКИ

Після перевірки підпису у верхньому меню доступні різні додаткові дії, зокрема::

- *Представити документ* - відображення оригіналу (підписаного) документа, якщо в системі встановлена програма для відображення даного типу документів.
- *Відкрити каталог* – відкриття перегляду каталогу на диску, де збережено документ.
- *Атрибути підпису* - показ додаткових даних, доданих до підпису.
- *Показати сертифікат* - відображення довідки з даними про особу, яка підписала документ. Є можливість експортувати сертифікат у форматі .crt за допомогою кнопки *Експортувати*.
- *Показати звіт xml* – показ звіту xml у вікні програми.
- *Створіть звіт у форматі PDF* - збереження читаного звіту (у форматі PDF) на диску з підтвердженням перевірки підпису.
- *Показати довідку* – буде відображено посібник користувача у форматі pdf.

Після правильної перевірки підпису можна створити розширені форми підпису¹:

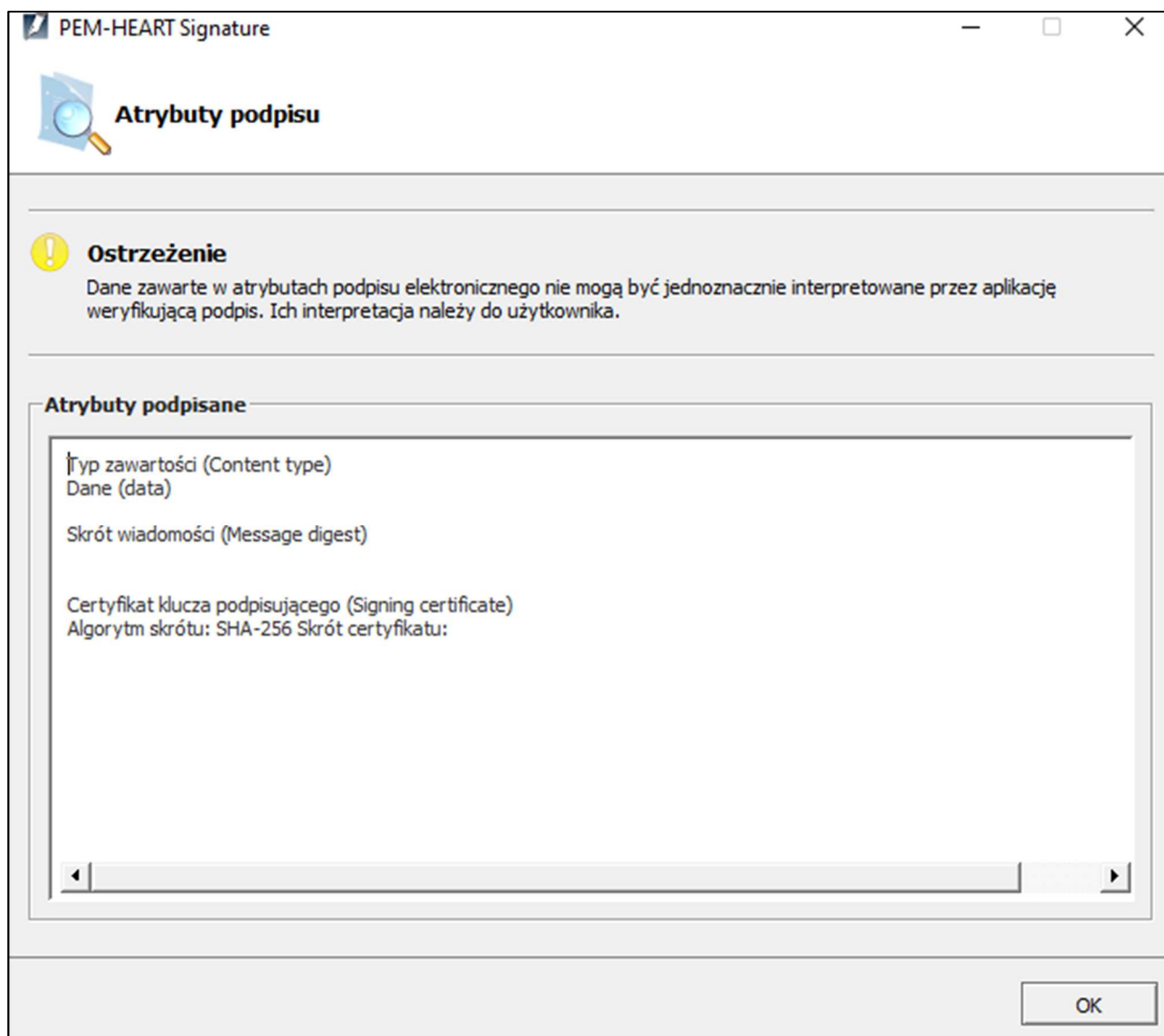
- *Створіть архівний персонаж* - забезпечення можливості коректної перевірки підпису на термін дії позначки часу (практично приблизно 7-10 років). Для створення архівної форми потрібен доступ до Інтернету та завантаження, серед іншого, дві часові позначки. Можливо, вам знадобиться придбати пакет часових позначок.

Термін дії архівної форми підпису можна продовжувати будь-яку кількість разів (шляхом додавання іншої позначки часу), кожного разу на наступні 7-10 років.

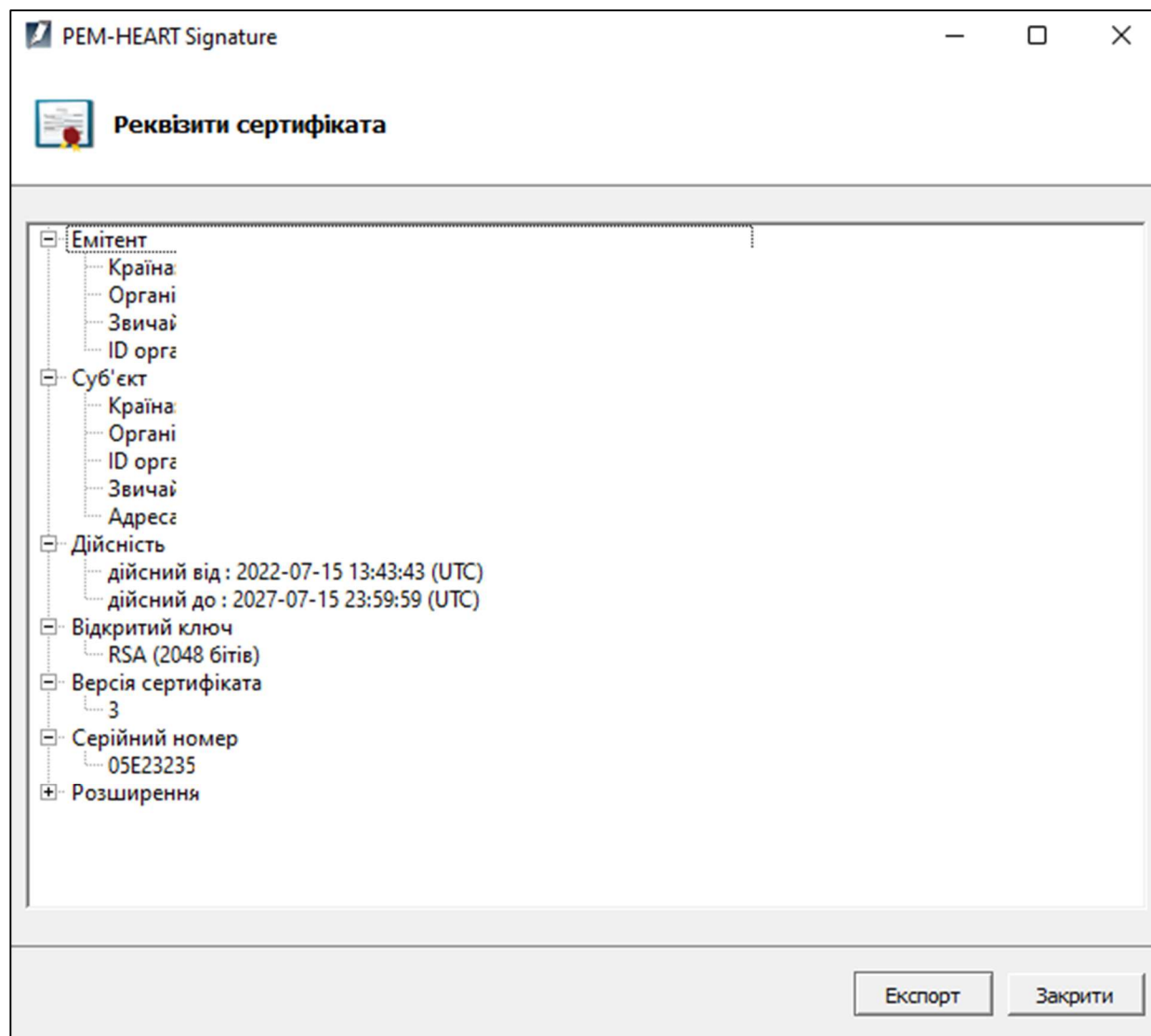
- *Створити довгу форму* - забезпечення можливості коректної верифікації підпису на термін дії ОЦСП і позначки часу (практично приблизно 5-10 років). Для створення довгої форми потрібен доступ до Інтернету та

1 У форматі підпису PAdES неможливо додати мітку часу до підпису, якщо вона не була додана відразу під час створення підпису

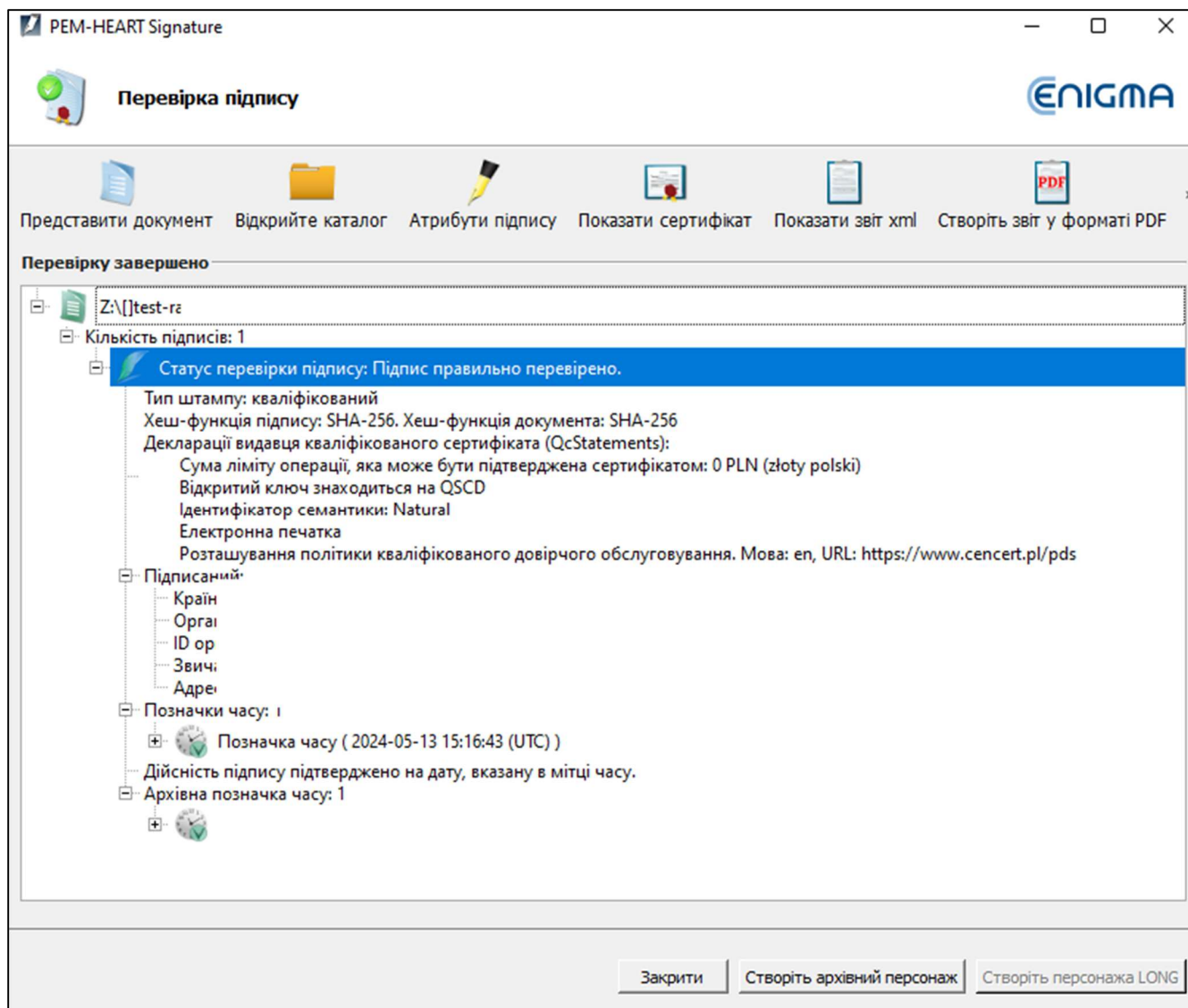
завантаження, зокрема: позначка часу. Можливо, вам знадобиться придбати пакет часових позначок.



Мал. 29 Вікно з атрибутами підпису



Мал. 30 Вікно з деталями сертифіката



Мал. 31 Статус підпису після перевірки

5 ОСНОВНІ ФУНКЦІЇ

5.1 ЗАПУСК ПРОГРАМИ

Усі функції програми доступні після запуску програми PEM-HEART *Signature* з меню *Пуск* (Windows) або з піктограми на робочому столі. В інших операційних системах запустить програму відповідно до вашої системи. Зовнішній вигляд програми такий же, як і в Windows.

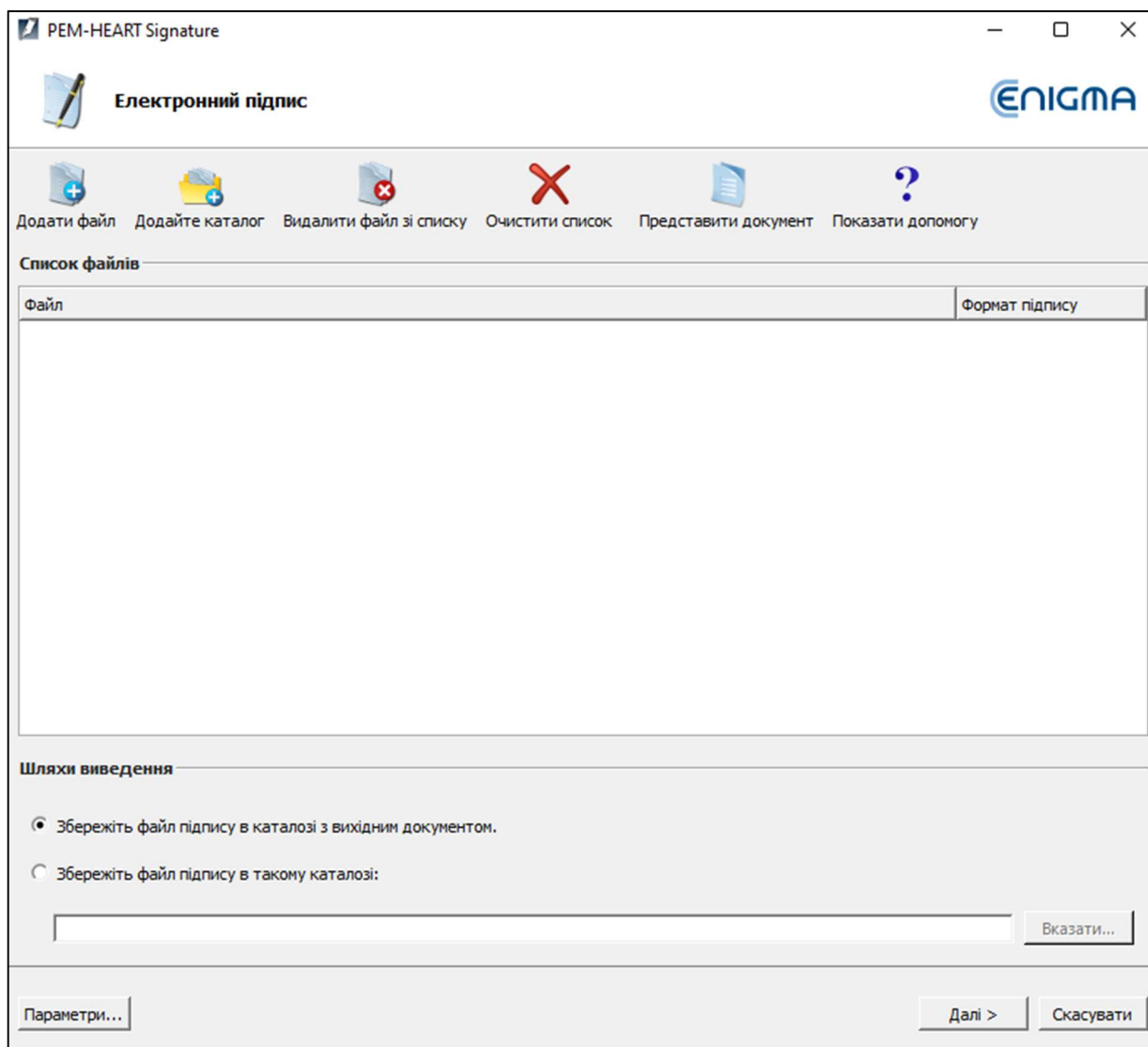
5.2 ПІДПИС У ПРОГРАМІ

5.2.1 ПОДАЧА ПІДПИСІВ – ПІДПИС НА КАРТЦІ АБО USB-ТОКЕНІ

Щоб підписати після запуску програми, клацніть значок *Підписати* (у лівій частині вікна, на панелі *Основні функції*). Відкриється вікно, у якому можна вибрати файли для підписання. Тут ви можете додати файл або файли, які потрібно підписати (кнопка *Додати файл*) або перетягнути файл у вікно списку файлів. Якщо вибрано весь каталог (кнопка *Додати каталог*), усі файли з цього каталогу та його підкаталогів буде додано до списку файлів для підпису. Після додавання всіх файлів до підпису натисніть *Далі*. Якщо до операційної системи підключено один зчитувач із сертифікатом, програма запитає PIN-код картки. Якщо зчитувачів із сертифікатами більше, програма відобразить вікно з вибором токенів. Після правильної операції буде створено підпис.



Мал. 32 Головне меню програми PEM-HEART Signature - вибір опції «Підписати»



Мал. 33 Вікно подачі електронного підпису

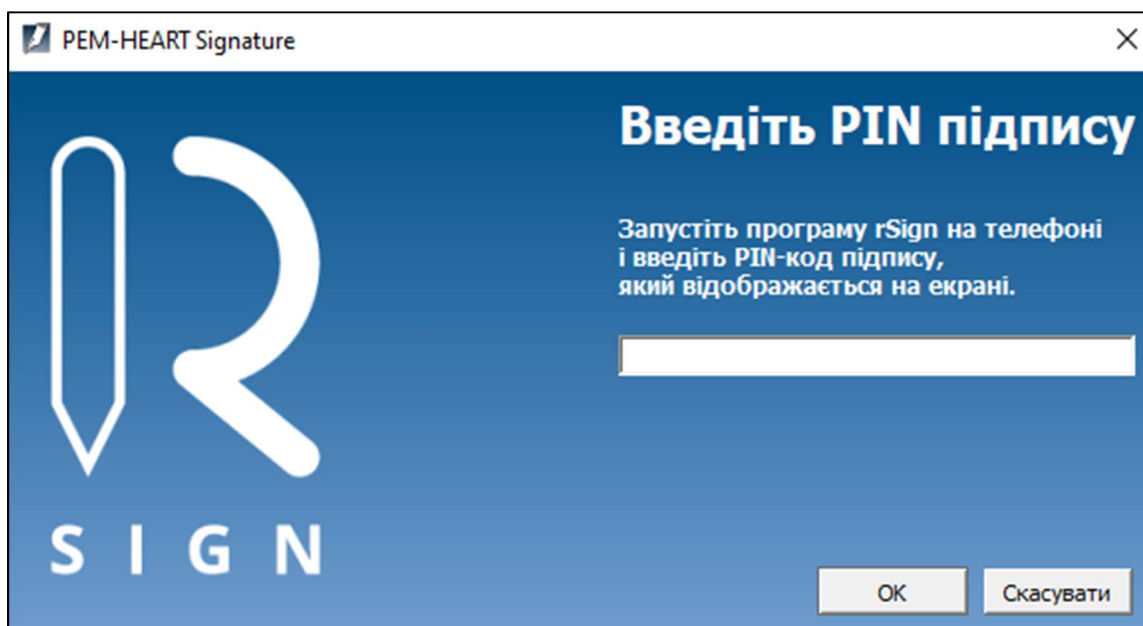
Коментарі:

- 1) Додаткові параметри, такі як зміна формату підпису, підпис в окремому файлі, відмітка часу та інші налаштування доступні під кнопкою *Параметри...*. Налаштування, змінені таким чином, застосовуються до конкретного підпису та не запам'ятовуються для подальшого використання. Дивіться також розділ **8.1 Зміна параметрів підпису**.
- 2) Залежно від формату підпису, підпис буде збережено в тому ж файлі без зміни імені або в новому файлі зі зміненим розширенням.

- 3) Якщо вибрати «підпис в окремому файлі», то підпис буде збережено в окремому файлі. У цьому випадку одержувачу необхідно надати два файли: вихідний файл і файл підпису.
- 4) Якщо підпис має містити мітку часу та/або відповідь OCSP, під час підпису потрібне підключення до Інтернету. Можливо, вам також знадобиться придбати послугу відмітки часу.

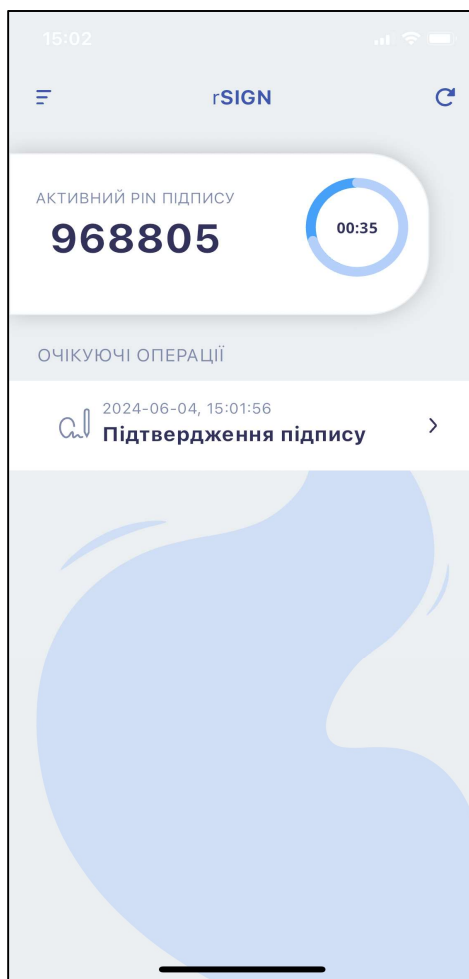
5.2.2 НАДСИЛАННЯ ПІДПИСІВ – ПІДПИС RSign (ХМАРНИЙ ПІДПИС)

Щоб підписати rSign, після запуску програми натисніть значок *Підписати* (у лівій частині вікна, на панелі *Основні функції*). Відкриється вікно, у якому можна вибрати файли для підписання. Тут ви можете додати файл або файли, які потрібно підписати (кнопка *Додати файл*) або перетягнути файл у вікно списку файлів. Якщо вибрано весь каталог (кнопка *Додати каталог*), усі файли з цього каталогу та його підкаталогів буде додано до списку файлів для підпису. Після додавання всіх файлів до підпису натисніть *Далі*. Після додавання всіх файлів до підпису натисніть кнопку *Далі*. Якщо до операційної системи підключено один зчитувач із сертифікатом, програма запитає PIN-код підпису. Якщо зчитувачів із сертифікатами більше, програма відобразить вікно з вибором токенів. Після правильної операції буде створено підпис.



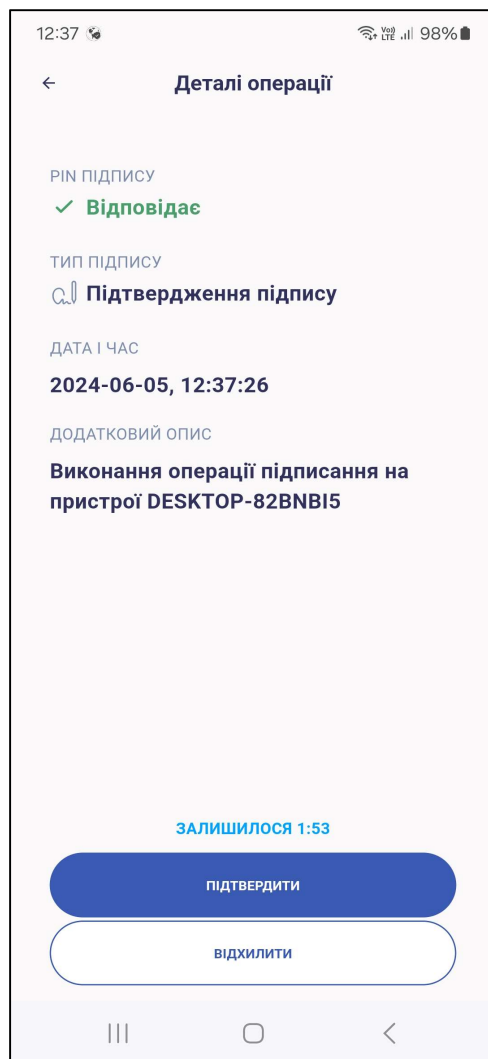
Мал. 34 Повідомлення щодо користування додатком rSign на телефоні

Тепер запустіть мобільний додаток *rSign by Cencert*, а потім прочитайте *Активний PIN-код для підпису* і скопіюйте його в програму на вашому комп'ютері та підтвердіть, натиснувши *OK*. Намір підписати необхідно підтвердити в додатку *rSign*.

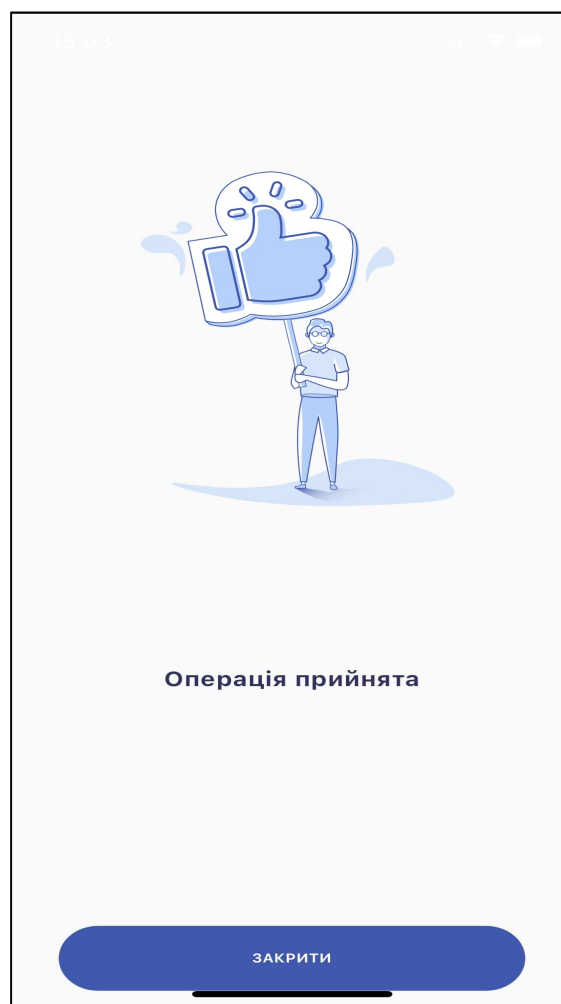
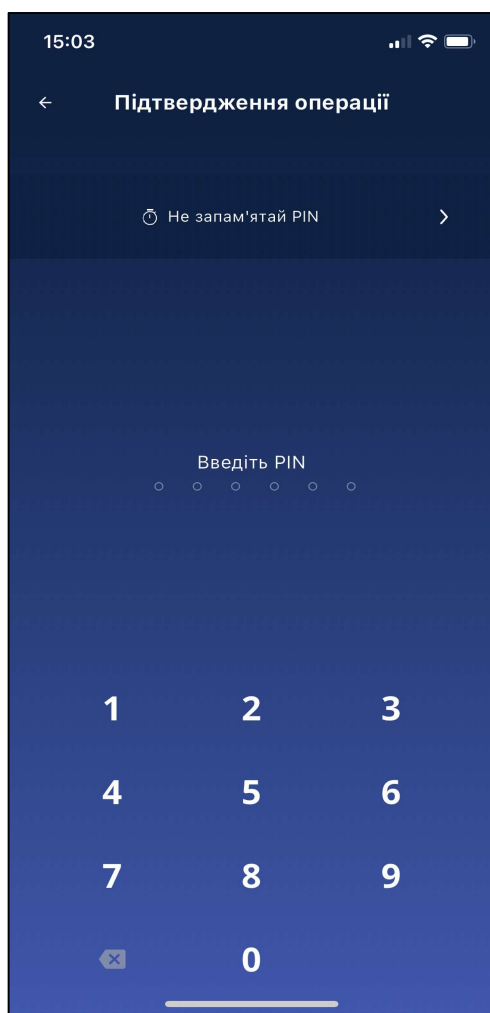


Мал. 35 Екран додатку rSign із активним PIN-кодом для підпису

У додатку ви повинні підтвердити свою готовність підписати, натиснувши кнопку *Підтвердження підпису* в розділі *ОПЕРАЦІЇ, ЩО ОЧІКУЮТЬСЯ*, прямо під відображенням Активним PIN-кодом для підпису. (**Мал. 35 Екран додатку rSign із активним PIN-кодом для підпису**). Якщо дані правильні, на наступному кроці підтвердіть операцію, натиснувши *ПІДТВЕРДИТИ* (**Мал. 36 Погодження на виконання операції електронного підпису**)

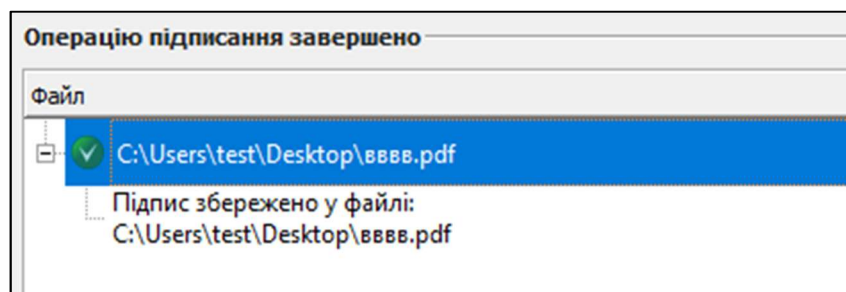


Мал. 36 Погодження на виконання операції електронного підпису



Мал. 37 Вікно для введення PIN-коду та підтвердження операції підпису (телефон)

Відобразиться екран для введення PIN-коду, дочекайтеся підтвердження операції - якщо код введено правильно, процедура буде прийнята, і з'явиться вікно, як показано на **Мал.37 Вікно для введення PIN-коду та підтвердження операції підпису (телефон)**.

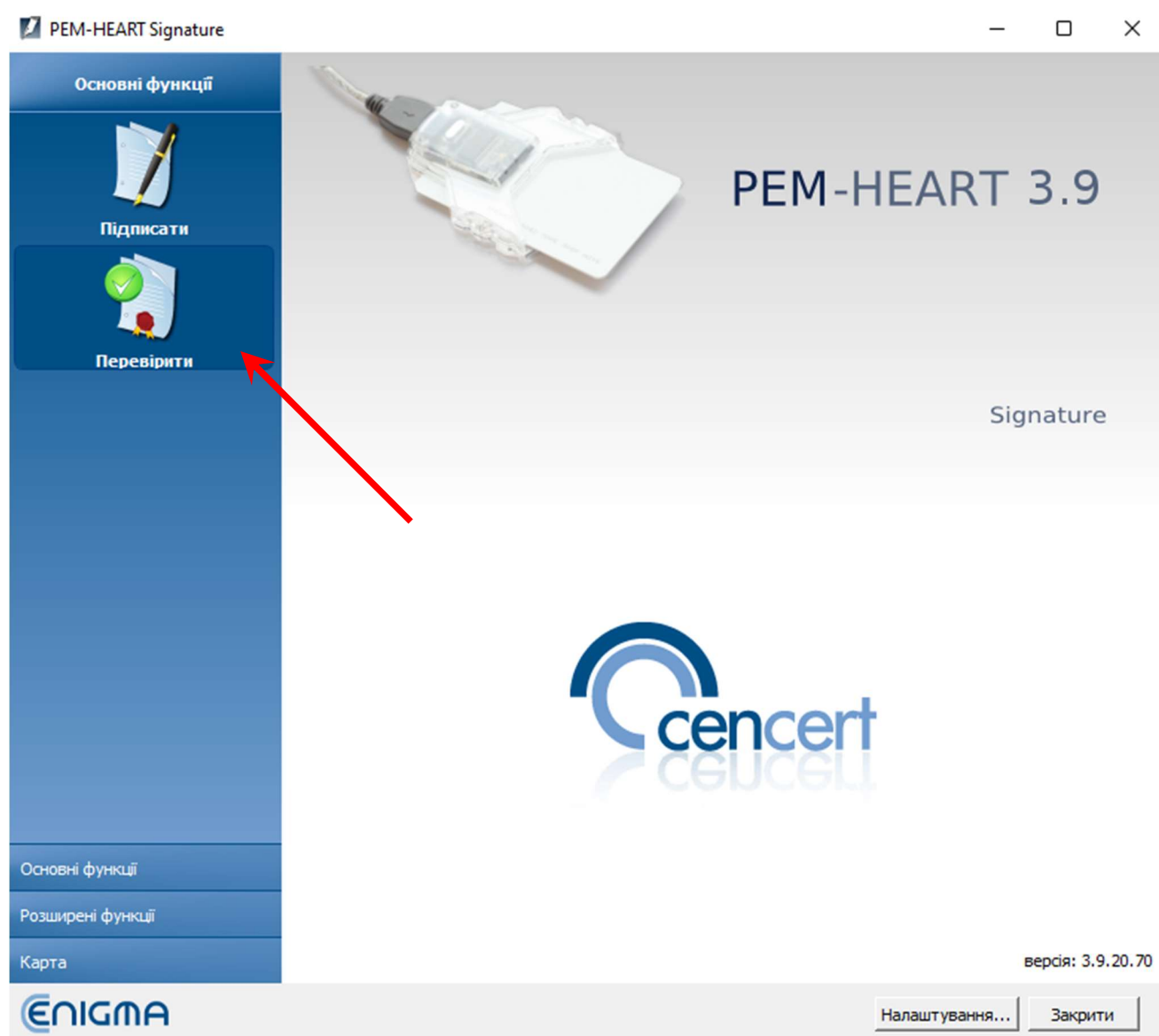


Мал. 38 Підтвердження операції підпису (комп'ютер)

Комп'ютерна програма відобразить інформацію про те, що документ успішно підписано (**Мал. 38 Підтвердження операції підпису (комп'ютер)**).

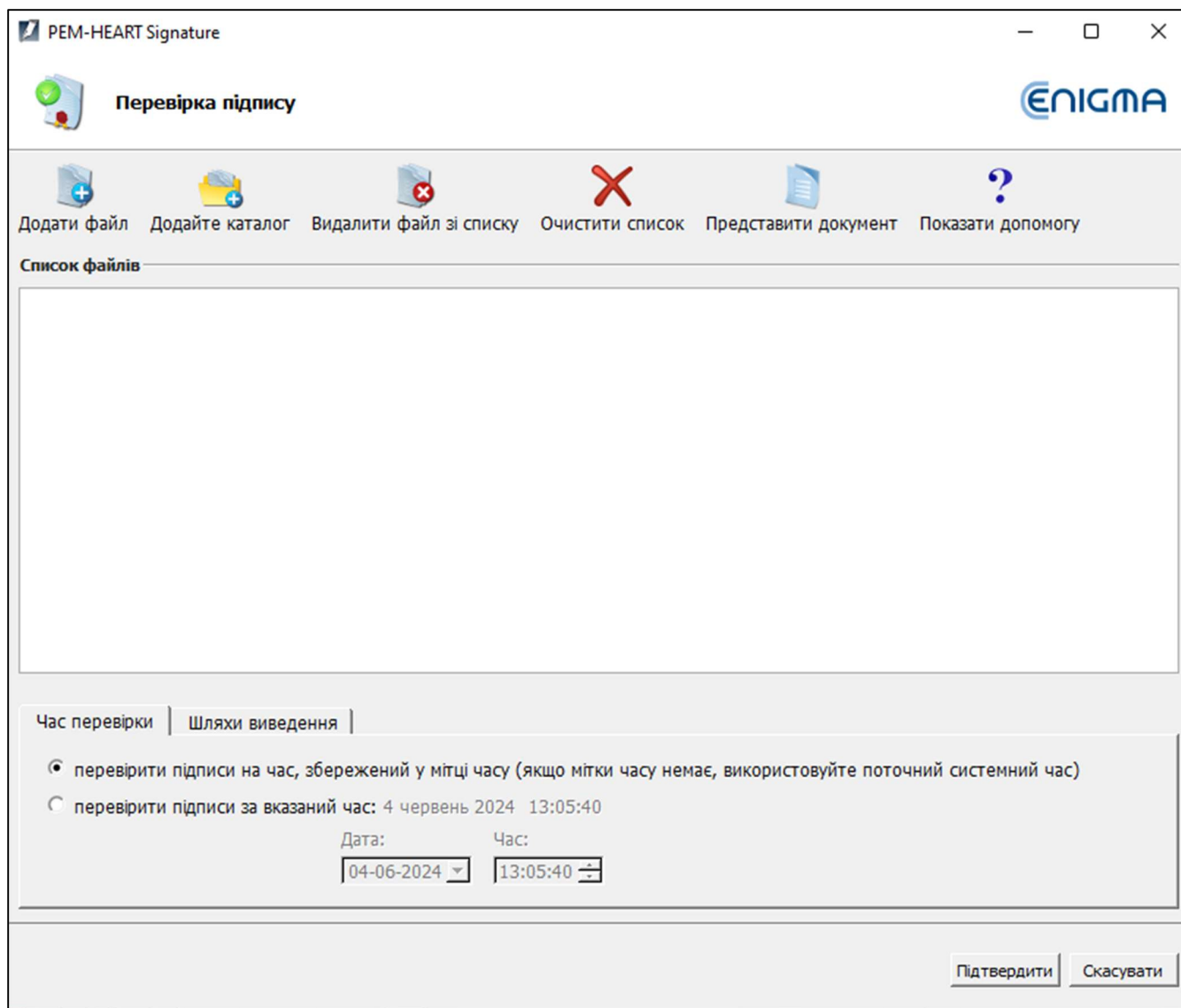
5.3 ПЕРЕВІРКА ПІДПISУ В ПРОГРАМІ

Щоб перевірити підпис, після запуску програми натисніть значок *Перевірити* (у лівій частині вікна, на панелі *Основні функції*).



Мал. 39 Головне меню програми PEM-HEART Signature - вибір опції «Перевірити»

Відкриється вікно, у якому можна вибрати файли для перевірки. Ви можете додати один чи декілька файлів для перевірки (кнопка *Додати файл*) або перетягнути файл у вікно списку файлів. Якщо вказано весь каталог (кнопка *Додати каталог*), програма включить усі файли з цього каталогу та його підкаталогів до списку файлів для перевірки. Після додавання всіх файлів натисніть кнопку *Перевірити*.

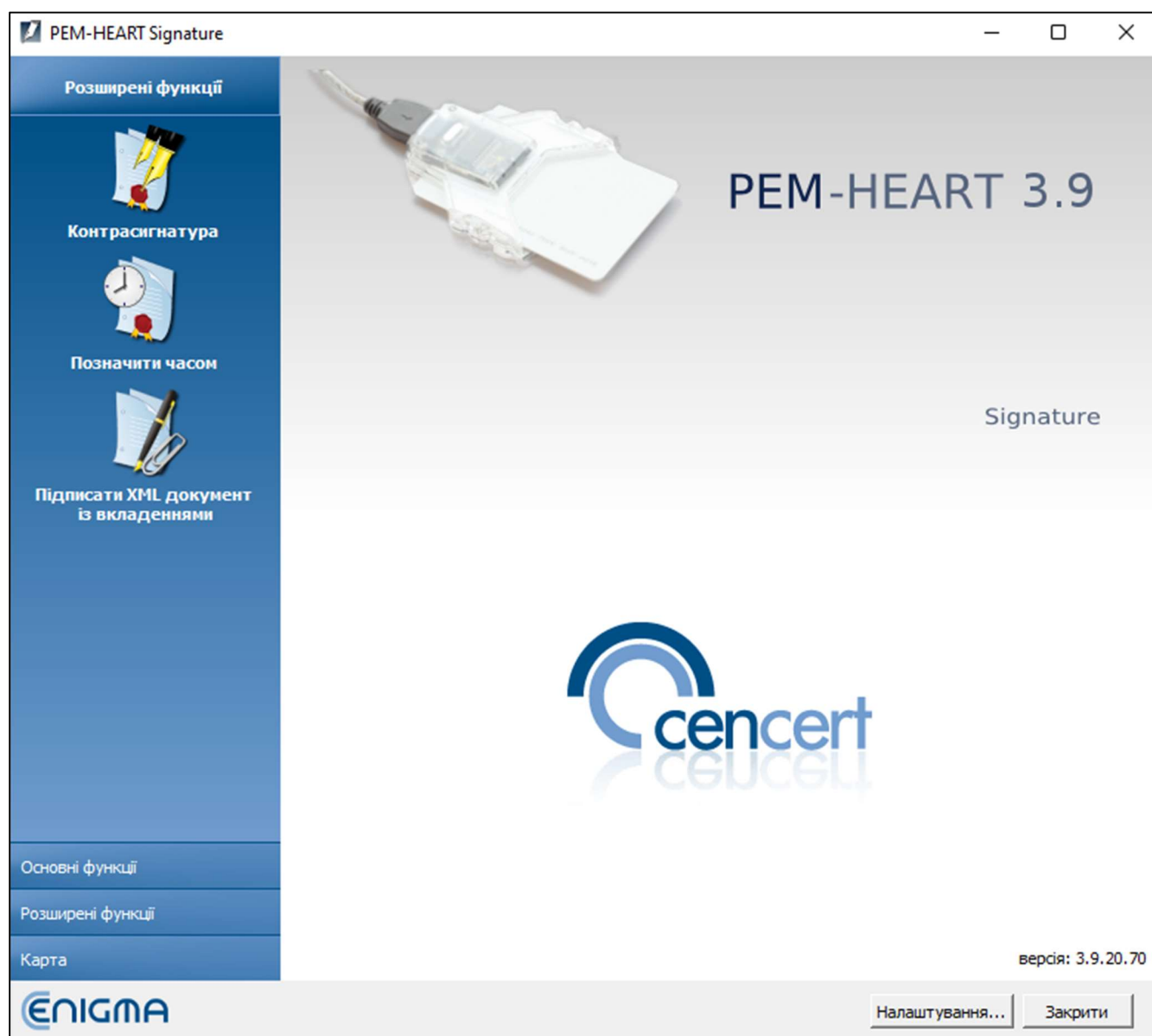


Мал. 40 Вікно перевірки електронного підпису

Програма перевірить підписи, збережені в документі, і відобразить результат перевірки.

Додаткову інформацію про перевірку можна знайти в [4.3 Перевірка підпису](#).

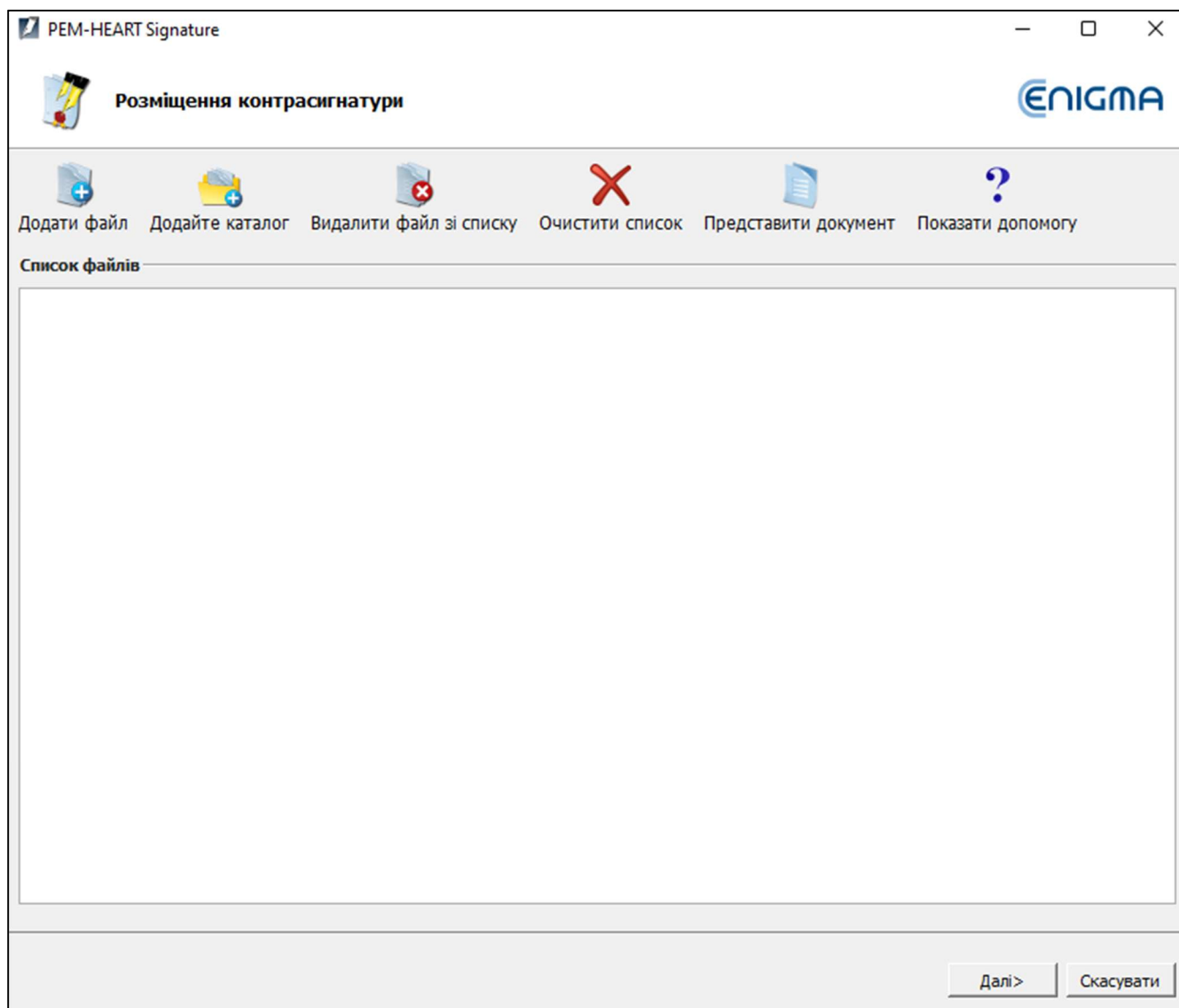
6 РОЗШИРЕНІ ФУНКЦІЇ



Мал. 41 Головне меню програми PEM-HEART Signature - розширені функції

6.1 КОНТРАСИГНАТУРА

Контрасигнатура — це особливий спосіб підпису, при якому технічно підпис ставиться не під самим документом, а під попередніми підписами (документ підписується опосередковано). Цей тип підпису запобігає видаленню попередніх підписів із документа. У випадку стандартних кількох підписів може бути технічно можливим видалити один із попередніх підписів із документа, зберігаючи дійсність решти підписів (*контрасигнація* унеможлиблює це).

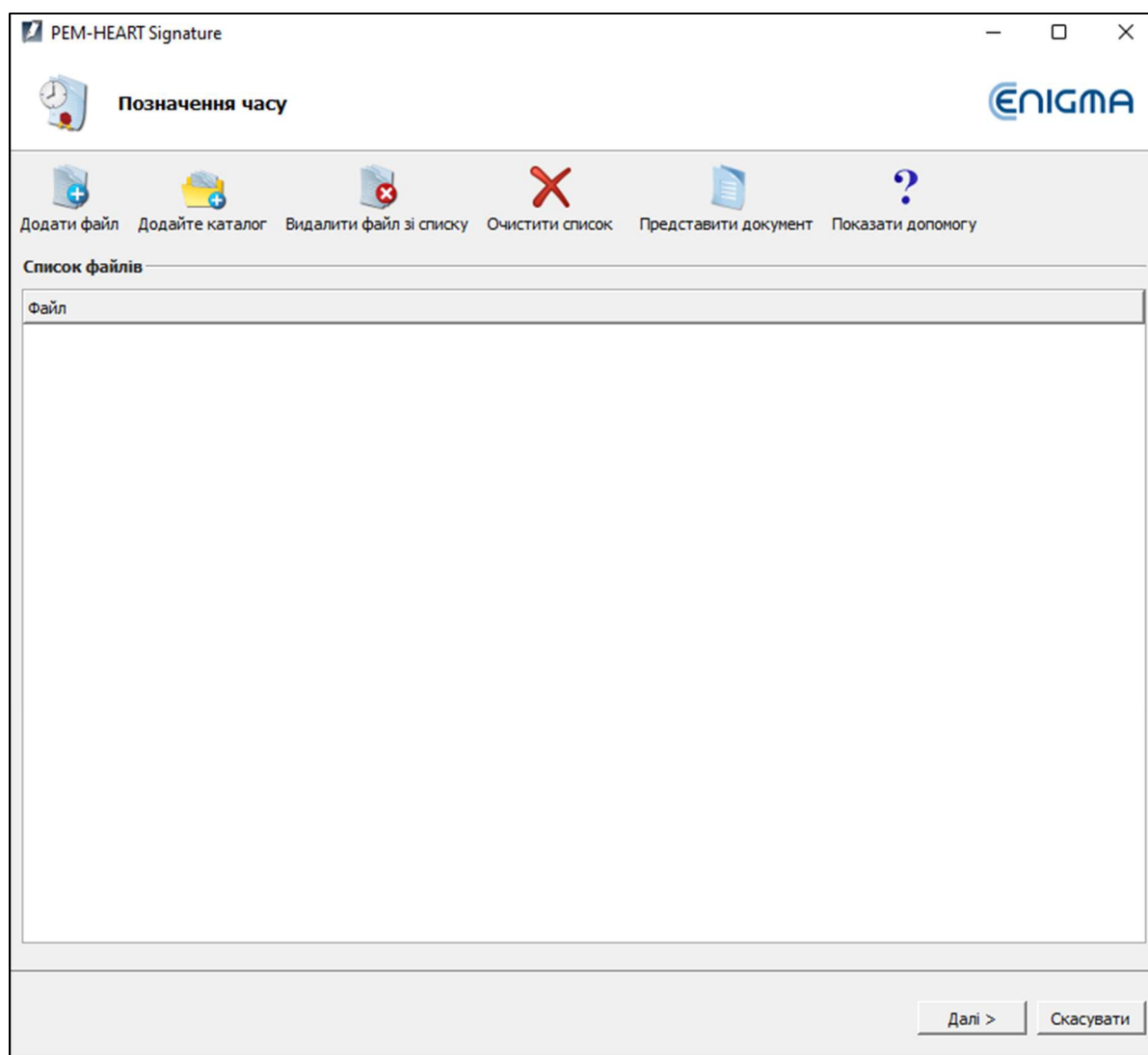


Мал. 42 Вікно подання контрпідпису

Термін вище значення не слід плутати з таким же терміном, який використовується в правовому обігу. Подання електронного підпису як «контрасигнація» (у сенсі, описаному вище) не дозволено законодавчими положеннями щодо електронних підписів. Застосовуються положення, що стосуються електронних підписів у цілому. У юридичному сенсі «контрасигнація», описаний у цьому документі, функціонує на тих самих принципах, що й будь-який інший електронний підпис..

6.2 ПОЗНАЧЕННЯ ЧАСУ

Кваліфікована позначка часу є доказом існування документа в певний час. У польському законодавстві судова дія з кваліфікованою позначкою часу має «певну дату». У всьому ЄС (згідно з регламентом eIDAS) кваліфікована електронна позначка



Мал. 43 Вікно для нанесення позначки часу на електронний підпис

часу має презумпцію точності дати й часу, які вона вказує, а також цілісності даних, з якими пов'язана зазначена дата й час.

Якщо для підпису використовується позначка часу, вона засвідчує не лише існування підписаного документа, але й сам підпис, що захищає від юридичних наслідків подальшого анулювання сертифіката, який використовувався для підпису.

Мітка часу також може бути додана до підпису пізніше, навіть одержувачем документа (насправді одержувач документа часто більше зацікавлений у можливості тривалої правильної перевірки підпису). Також варто розглянути більш просунуті форми підпису - тобто *long* та *архівну* (див. гл. [4.3.1 Панель перевірки](#)). Ці форми також можуть використовувати мітки часу, але вони доповнюють їх іншими даними, необхідними для перевірки.

Виберіть *Додаткові функції* в меню (панель у лівій частині головного вікна) і натисніть піктограму *Мітка часу*.

Відкриється вікно, у якому можна вказати файли та/або каталоги, як під час підписання та перевірки підпису. Після вибору файлів і натискання кнопки *Далі* програма запитує PIN-код картки (щоб підписати запит про відмітку часу) або PIN-код rSign, а потім додає позначку часу до кожного підпису, що міститься у цьому файлі.

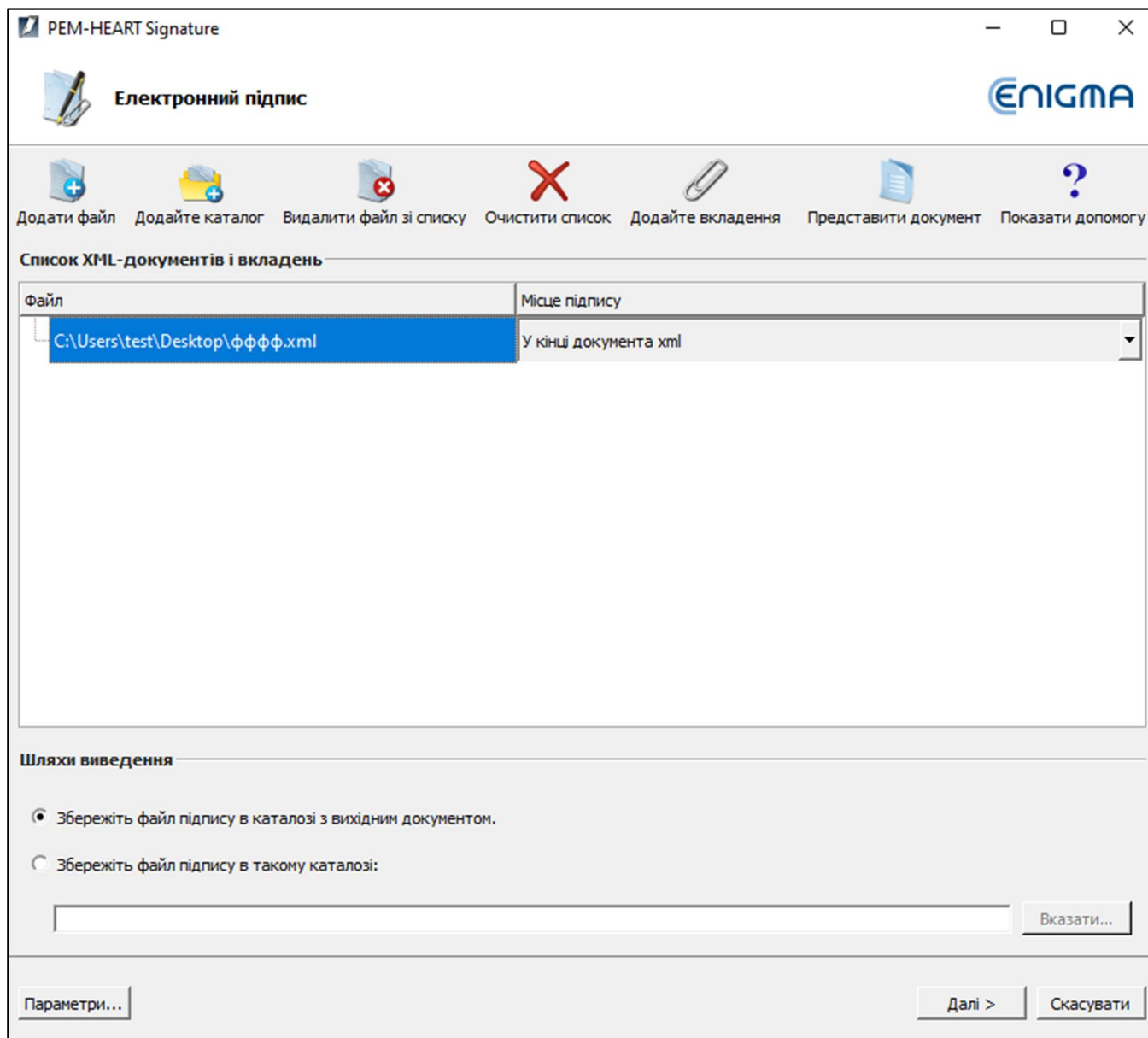
Увага: Для завантаження часових позначок може знадобитися придбати пакет часових позначок.

6.3 ПІДПИСАННЯ XML-ДОКУМЕНТА З ВКЛАДЕННЯМИ

За замовчуванням, коли програма підписує XML-документ за допомогою підпису в оточенні (*XAdES enveloped*), вона розміщує підпис у кінці структури документа. У переважній більшості випадків така поведінка програми є достатньою та відповідає вимогам систем, що використовують підписи. Однак, якщо є потреба розмістити підпис всередині документа інакше, скористайтеся опцією *Підписати XML-документ із вкладеннями*. Використання цього параметра призначене для досвідчених користувачів і вимагає знання структури *XML-файлів*, зокрема знання документації *XML Pointer Language (XPointer)*.

Виберіть вкладку *Додаткові функції* в меню (панель у лівій частині головного вікна) і натисніть піктограму *Підписати XML-документ із вкладеннями*. Коли програма відобразить вікно для додавання файлів до підпису, виберіть XML-файл (додатково

файл може вказувати вкладення). Якщо підпис має бути розміщено в місці, відмінному від кінця файлу, потрібно вказати відповідне місце в структурі документа XML. У такому випадку користувач має вибрати опцію *Додати новий...* у розділі *Місце підпису*, у якому відобразиться вікно налаштування місця підпису.



Мал. 44 Підписання XML-документа з вкладеннями - перехід до налаштування розташування підпису

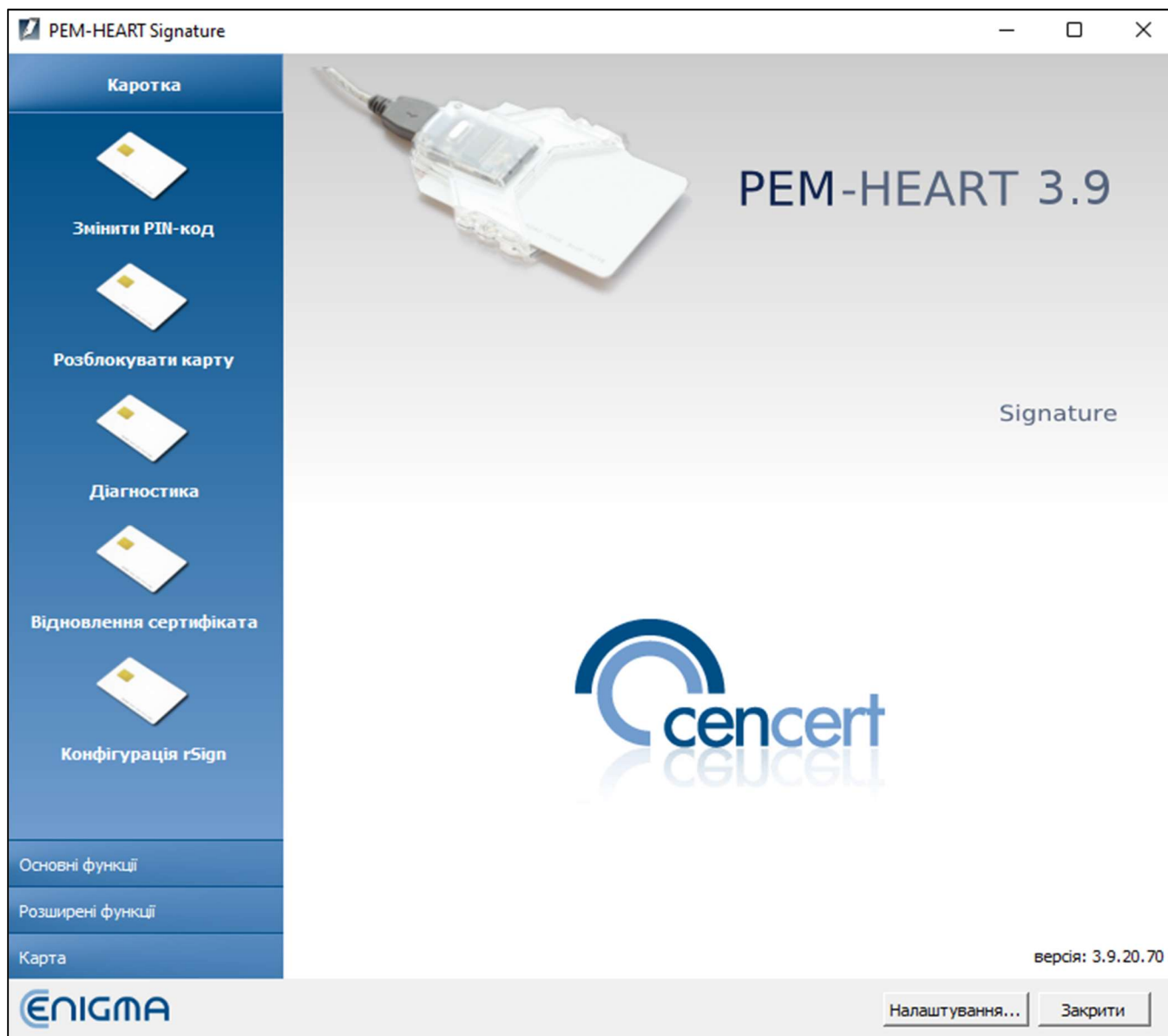
Потім у наступному вікні натисніть кнопку , введіть назву вашої конфігурації, надайте структуру *xpointer* і, якщо необхідно, опис конфігурації, що визначається. Структура *xpointer* визначається як: *xpointer*([вказує на вузол XML]). Доступні форми вказівки цього місця описано в документації *XML Pointer Language (XPath)*, доступній, зокрема, за адресою: на сторінках <http://www.w3.org/TR/WD-xptr>.

Після завершення підписання з'явиться вікно підсумків. Створення підпису у форматі XAdES в оточенні (*XAdES enveloped*) не змінює розширення файлу *XML* або його структуру.

7 ПІДТРИМКА КРИПТОГРАФІЧНИХ КАРТ У ПРОГРАМІ

7.1 ЗМІНА PIN-КОДУ

(Функція недоступна для підпису *rSign*) Щоб змінити PIN-код картки, виберіть у головному меню вкладку *Картка* (панель у лівій частині головного вікна) і клацніть значок *Змінити PIN*.

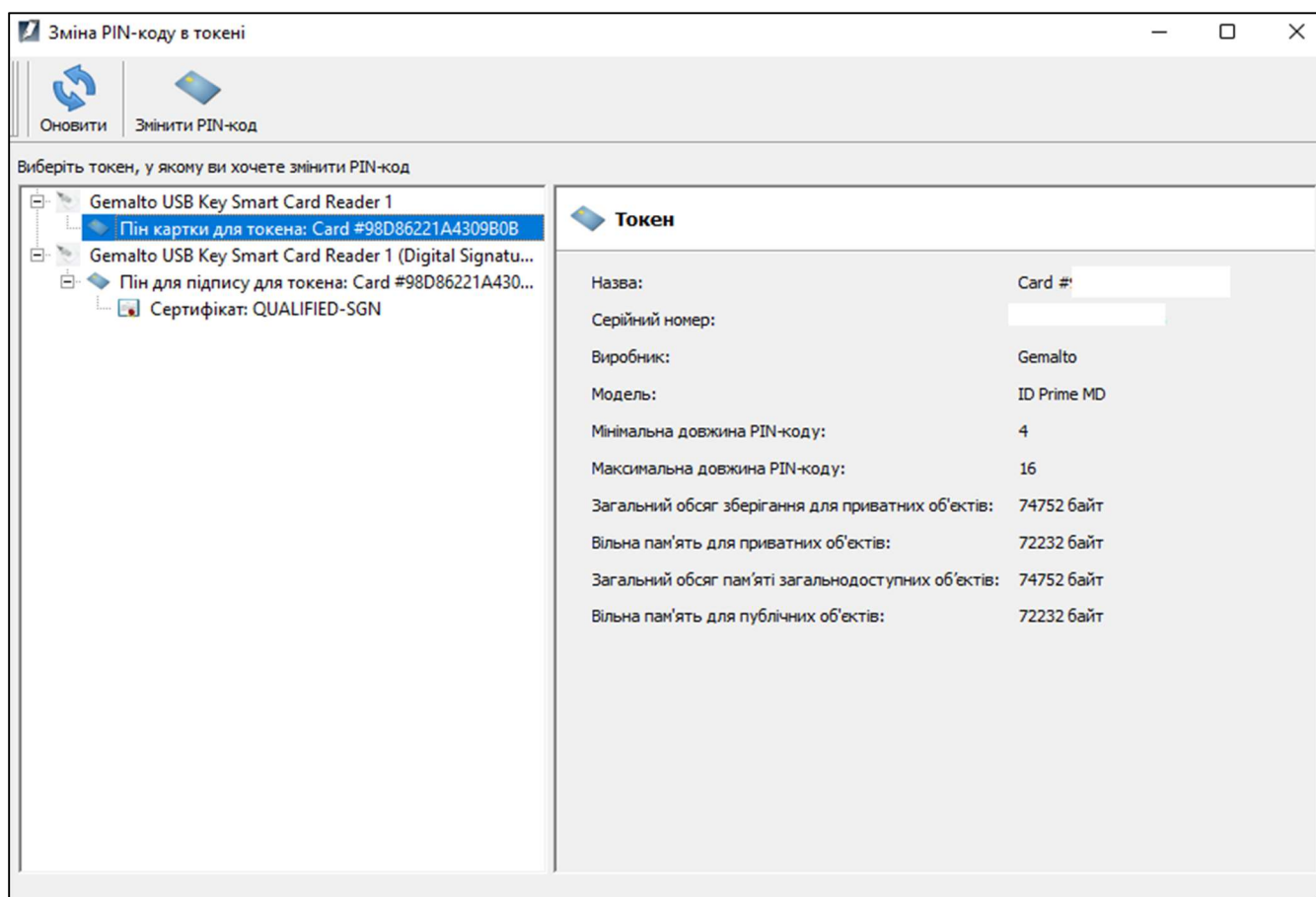


Мал. 45 Головне меню програми PEM-HEART Signature - вибір вкладки «Картка»

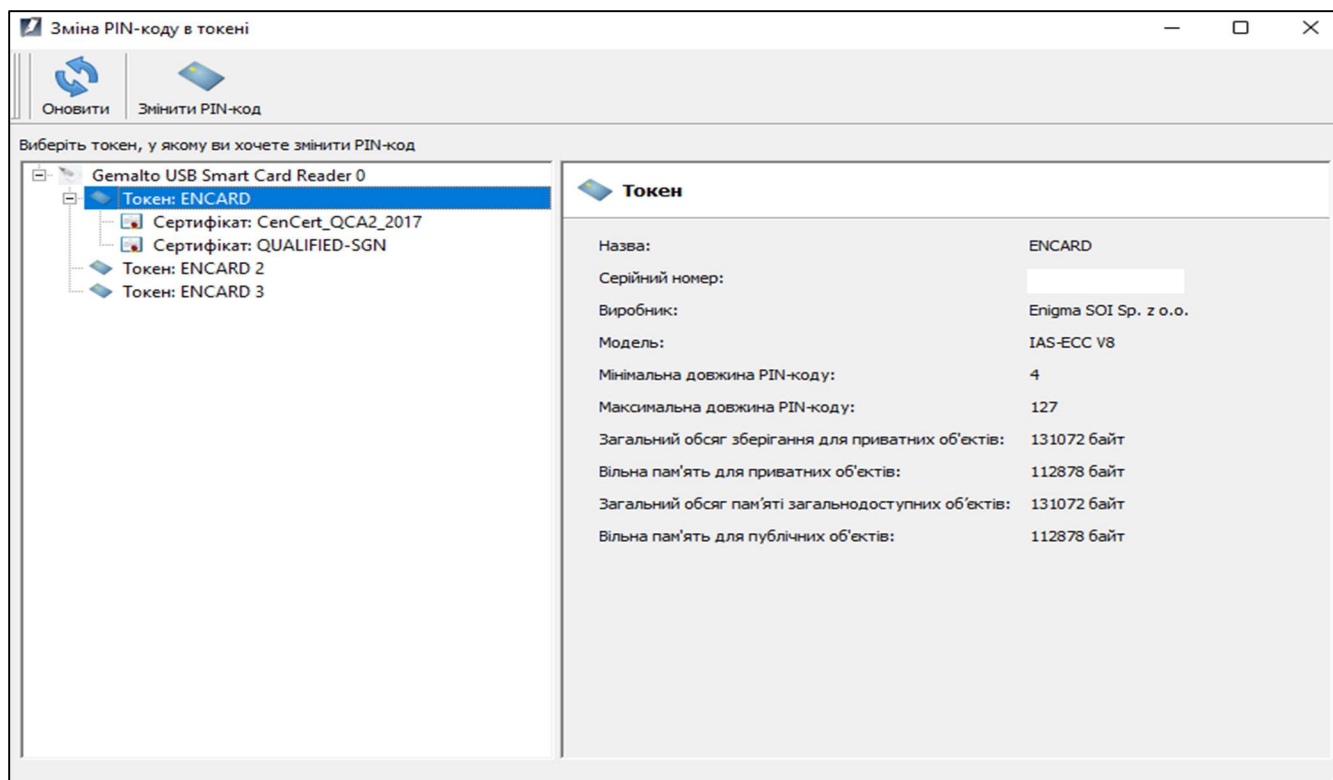
Потім потрібно вказати токен, для якого потрібно змінити PIN-код.

Увага:

- Для карт IDEMIA: об'єкти, пов'язані з кваліфікованим підписом, завжди розміщуються в першому зверху жетоні; інші токени можна використовувати для інших цілей, наприклад, для електронної печатки.
- Для карток IDPrime: об'єкти, пов'язані з кваліфікованим підписом, завжди розміщуються на другому зверху токени – він називається „Digital Signature PIN”.



Мал. 46 Зразок екрана програми для карти Thales типу A



Мал. 47 Зразок екрана програми для IDEMIA Encard

Щоб внести зміни, користувач вибирає опцію «Змінити PIN», розташовану над списком токенів. Щоб змінити код, необхідно ввести правильний поточний PIN-код і двічі ввести новий код. Не рекомендується використовувати для PIN-коду польські літери чи інші символи, які можуть бути неправильно введені через різні мовні налаштування клавіатури комп'ютера (картка блокується після 3 спроб введення неправильного коду). ПІН-код рекомендується записувати в надійному місці (окремо від картки), виняток становить ПІН для карток thales (перший токен), в цьому випадку він буде заблокований після 5 спроб.

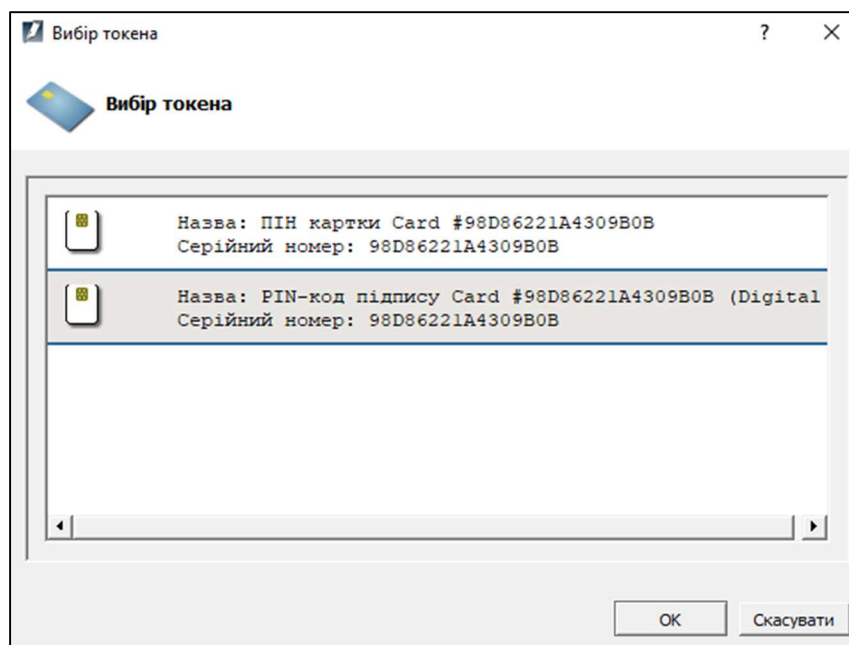
Мал. 48 Екран зміни PIN-коду картки
IDEMIA

Увага! Якщо PIN-код заблоковано, картку можна розблокувати лише за допомогою PUK-коду.

PIN/PUK-коди призначаються користувачем при активації картки. Cencert не має PIN/PUK-кодів, і не може розблокувати картку через неправильний PIN/PUK-код.

7.2 РОЗБЛОКУВАННЯ КАРТИ

(Функція недоступна для *rSign*) Якщо картку було заблоковано після введення забагато неправильних PIN-кодів, її можна розблокувати за допомогою PUK-коду. PUK-код призначається користувачем при активації картки. Після використання кнопки *Розблокувати картку* відкриється вікно з вибором токенів.



Мал. 49 Розблокування карти - вибір токена - картка IDPrime

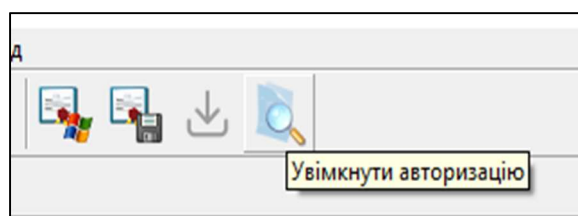
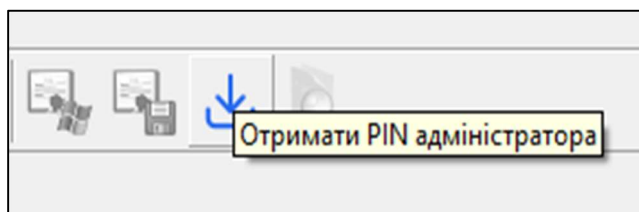
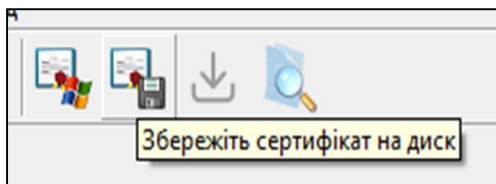
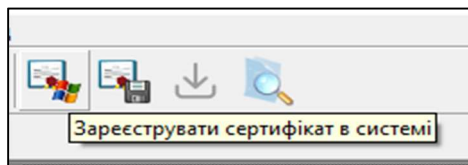
Після правильного введення PUK-коду можна буде встановити новий PIN-код і картку буде розблоковано.

Увага! Існує обмежена кількість спроб розблокувати картку за допомогою PUK-коду. Якщо дані заповнюються неправильно під час кожної спроби, картка блокується назавжди, і її неможливо використовувати далі.

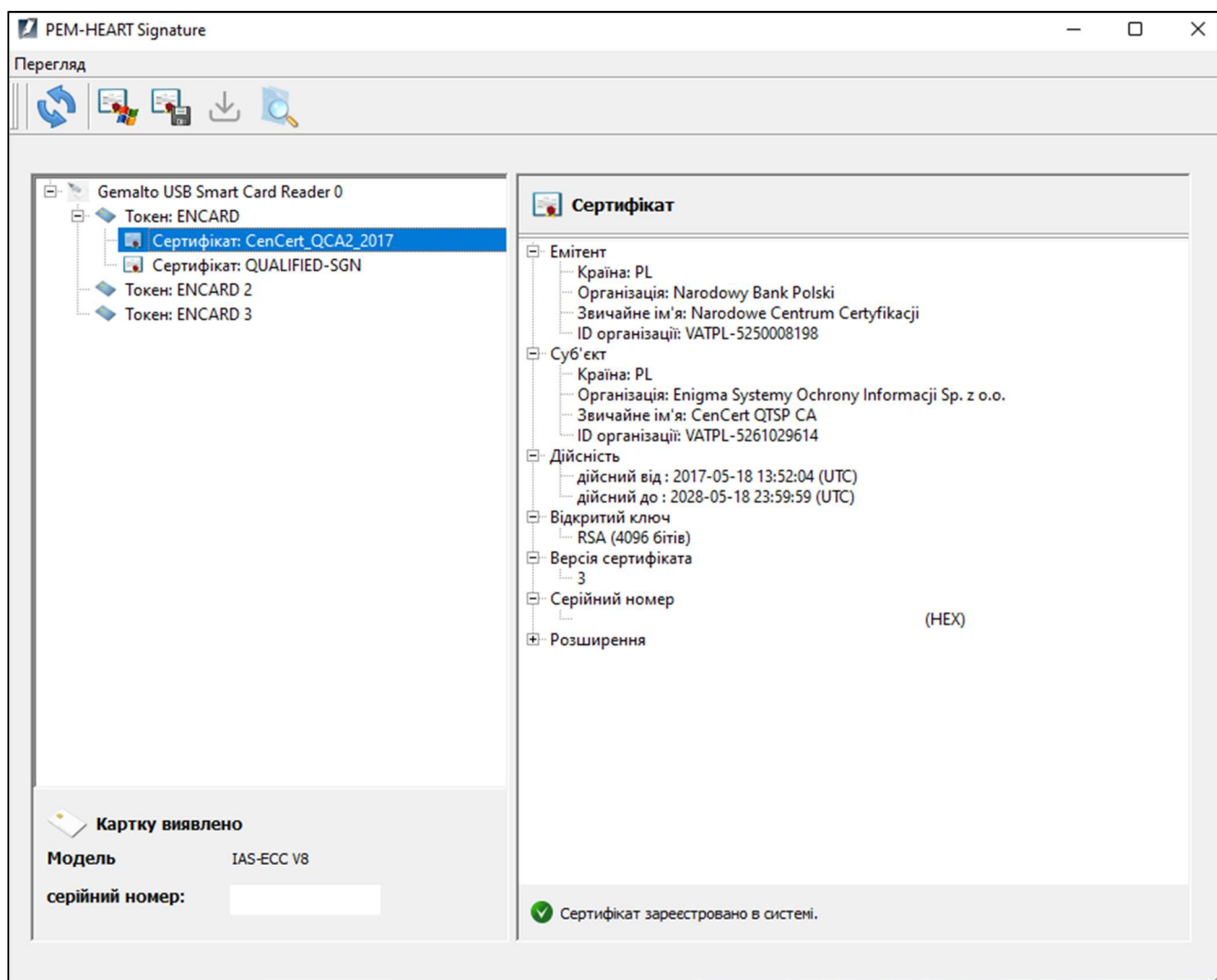
PIN/PUK-коди призначаються користувачем при активації картки. Centert не має PIN/PUK-кодів і не може допомогти, якщо вашу картку заблоковано через неправильний PIN/PUK-код.

7.3 ДІАГНОСТИКА

Панель *Діагностика* показує додаткову інформацію про дані сертифіката, дозволяє зберегти сертифікат у файл, зареєструвати його в Windows, завантажити PIN-код адміністратора (тільки для карток IDPrime) і увімкнути журналювання (лише для карток IDEMIA та rSign – функція описана в розділі **10.1 Журнали роботи карток для систем Windows**).



Мал. 50 Додаткові параметри на екрані Діагностики



Мал. 51 Вигляд відкритої панелі Діагностики - відображення токена з картки та rSign

7.4 ДОДАТКОВІ ОПЦІЇ

7.4.1 ВІДНОВЛЕННЯ СЕРТИФІКАТА

Вас буде перенаправлено та ви відкриєте *Програму відновлення сертифіката PEM-HEART*. Посилання на сторінку посібника користувача: <https://www.cencert.pl/poradnik-uzytownika/>

7.4.2 КОНФІГУРАЦІЯ RSIGN

Програма налаштування PEM-HEART rSign буде перенаправлена та відкрита

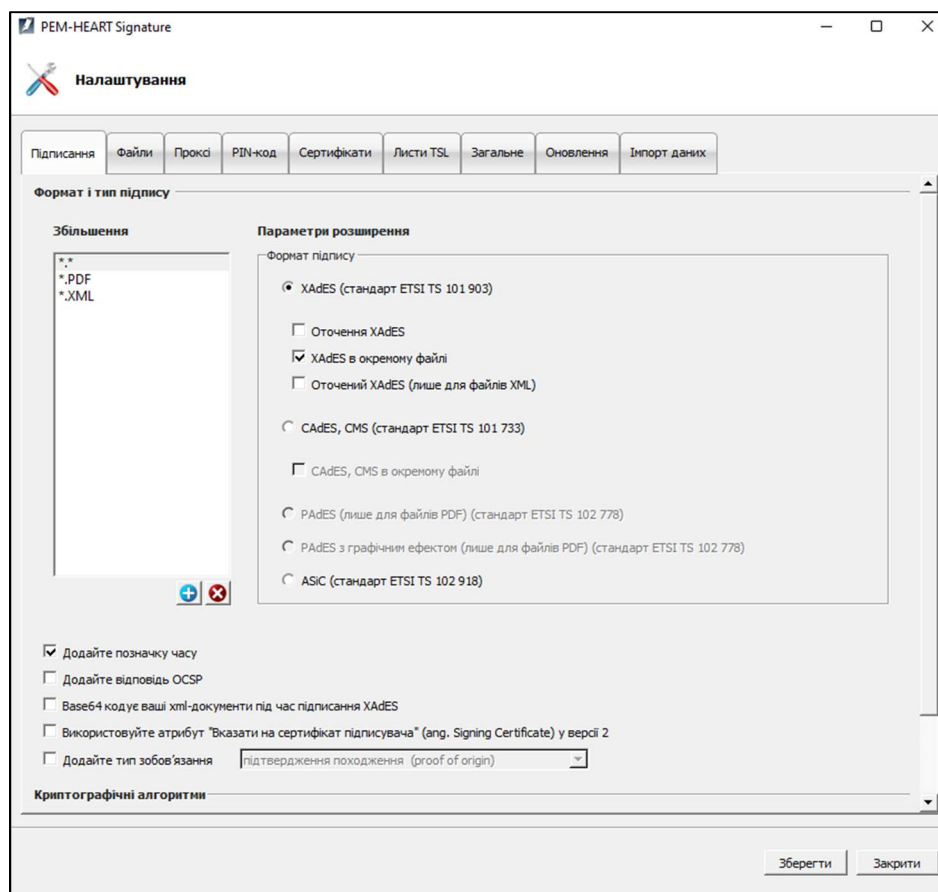
8 НАЛАШТУВАННЯ ПРОГРАМИ

Увага!

Усі операції зміни параметрів будуть збережені в пам'яті програми після їх збереження за допомогою кнопки *Зберегти* в нижньому правому куті меню програми.

8.1 ЗМІНА ПАРАМЕТРІВ ПІДПISУ

Щоб змінити параметри підпису, у головному вікні програми натисніть кнопку **Налаштування** (знаходиться в нижньому правому куті екрана програми, поруч із кнопкою **Закрити**). З'явиться нове вікно налаштувань із відкритою вкладкою **Підпис**. Усі параметри, що визначають формат підпису (XAdES, CAdES, PAdES, ASiC) буде застосовано до файлів із розширенням, вибраним у списку Розширень. Всі файли з розширеннями *.* (тобто всі файли, окрім тих, які визначені у списку під цим розширенням) буде підписаний за замовчуванням у форматі XAdES в окремому файлі. Водночас файли *.PDF і *.XML мають власні формати підпису за замовчуванням, які буде видно після вибору відповідного рядка у списку *.PDF або *.XML.



Мал. 52 Вікно для зміни параметрів підпису

Тут можна додати (або видалити) розширення файлів (за допомогою значків  і ), для яких має використовуватись інший формат підпису за замовчуванням. Наприклад, додавши новий елемент „*.docx” і визначивши, що для цих файлів потрібно зробити підпис, наприклад, CAdES і CMS в окремому файлі, щоб ініціювати підпис для кожного файлу з документом Ms Word. (*.docx), програма за замовчуванням запропонує підпис у форматах CAdES і CMS в окремому файлі.

У розділі нижче щодо вибору розширення та встановлення формату підпису для певного розширення є додаткові параметри для підписів. Ці параметри застосовуються до всіх підписів – незалежно від імені файлу.

Параметр *Додати мітку часу* означає, що мітка часу буде додано до кожного підпису (**Увага!** Для належної роботи вам може знадобитися придбати пакет часових позначок).

Параметр *Додати відповідь OCSP* означає, що окрім мітки часу (галочка *Додати мітку часу* відкриває можливість вибрати *Додати відповідь OCSP*), інформація про статус сертифіката, який використовується для підпису, буде додано до підпису

(таким чином створюється підпис у формі long – див. також розділ **4.3.1 Панель перевірки**).

Параметр *Кодування base64 документів xml при створенні навколишнього підпису XAdES* необхідний у особливих ситуаціях, коли система перевірки підписаних документів має обмежені можливості для перевірки різних форматів підписів і вимагає цього.

Параметр *Використовуйте атрибут «Показник сертифіката підписувача»*. (*ang. Signing Certificate*) у версії 2 призводить до того, що підпис включає вказівку сертифіката у форматі, який відповідає новим версіям стандартів ETSI щодо формату підпису. Будь ласка, виберіть цей параметр, якщо він потрібен системі перевірки підпису, яка використовує лише нові формати.

Вибір параметра *Додати тип зобов'язання* додає підписаний атрибут, який вказує, з якою метою (в якій ролі) підписувач підписав підпис (наприклад, як «офіційне затвердження», «підтвердження отримання» тощо).

Параметр *Алгоритм* визначає криптографічний хеш-алгоритм, який використовується для видачі підпису. Програма дозволяє вибирати лише хороші алгоритми, які гарантують відповідну безпеку (якщо дана версія програми актуальна).

8.2 ФАЙЛИ

Вкладка містить параметри налаштування вихідних каталогів для оброблених документів. За замовчуванням програма обробляє документи в тому ж каталозі, де знаходиться документ. Можна визначити інші каталоги, де будуть зберігатися підписані або перевірені документи.

Щоб визначити каталог, поставте позначку перед описом параметра. Після цього буде активовано кнопку *Вказати*, за допомогою якої можна вказати певний каталог у файловій системі.

The screenshot shows the 'Налаштування' (Settings) window with the 'Вихідні каталоги' (Output folders) tab selected. The tab bar includes: Підписання, Файли, Проксі, PIN-код, Сертифікати, Листи TSL, Загальне, Оновлення, and Імпорт даних. Under the 'Вихідні каталоги' section, there are two checkboxes:

- ☐ При підписанні розмістити отримані документи у вказаному каталозі :
- ☐ Розмістіть перевірені документи у вказаному каталозі:

 Each checkbox has an empty text input field followed by a 'Вказати...' (Specify...) button.

Мал. 53 Визначення вихідних каталогів для оброблених документів

8.3 ПРОКСІ

Вкладка використовується для визначення підключення до проксі-сервера. Є дві можливі конфігурації на вибір:

- Використовуйте налаштування системи (тільки для систем Windows) – параметр за замовчуванням, конфігурація завантажується з налаштувань

The screenshot shows the 'Налаштування' (Settings) window with the 'Проксі' (Proxy) tab selected. The tab bar is the same as in the previous image. Under the 'Проксі-сервер' (Proxy server) section, there is a checked checkbox:

- ☒ Використовуйте налаштування системи

Мал. 54 Проксі-сервер - налаштування системи

системи (реєстру)

- Налаштувати проксі – ручне налаштування конфігурації із зазначенням адреси порту та/або даних для аутентифікації. Заповніть усі обов'язкові поля для даного проксі-сервера. Активація налаштувань підтверджується кнопкою Зберегти в нижньому правому куті програми. Аутентифікація проксі є додатковою версією і не є обов'язковою

Неправильна конфігурація сервера призводить до відсутності доступу програми до Інтернету (неможливо завантажити мітку часу, може бути неможливо перевірити підписи).

Підписання Файли **Проксі** PIN-код Сертифікати Листи TSL Загальне Оновлення Імпорт даних

Проксі-сервер

☐ Використовуйте налаштування системи

Налаштування проксі

☒ Налаштувати проксі

Конфігурація проксі

Проксі HTTP:

Порт:

☒ Аутентифікація проксі

Аутентифікація проксі

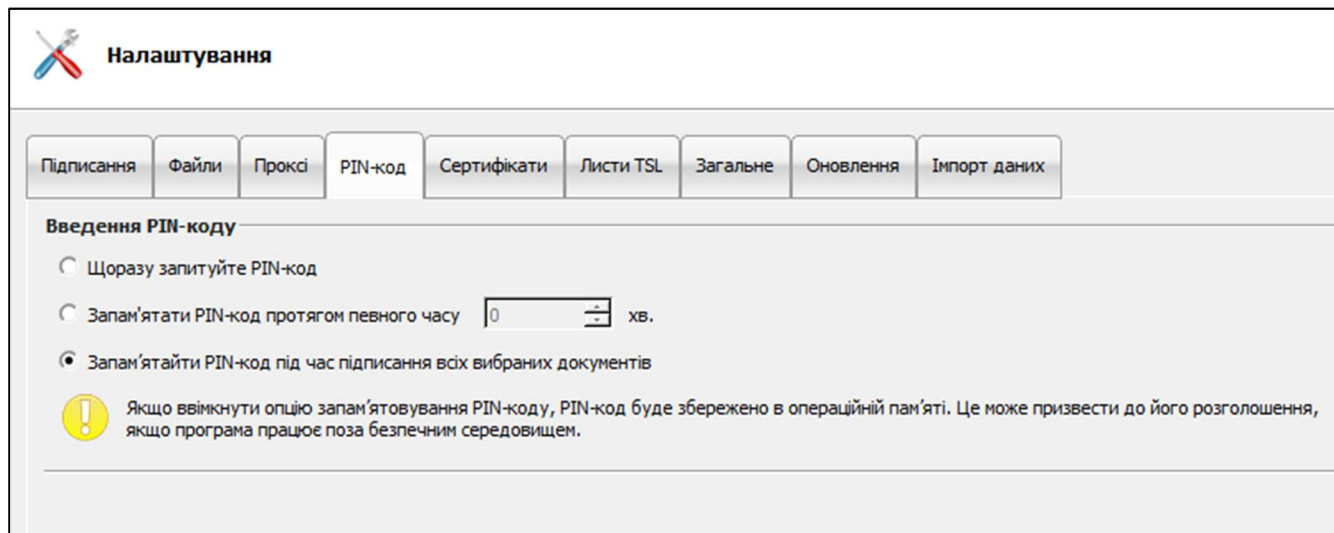
Назва користувача:

Пароль:

Мал. 55 Проксі-сервер - налаштування вручну

8.4 PIN

Вкладка PIN-коду використовується для встановлення параметрів



Мал. 56 Налаштування PIN-коду

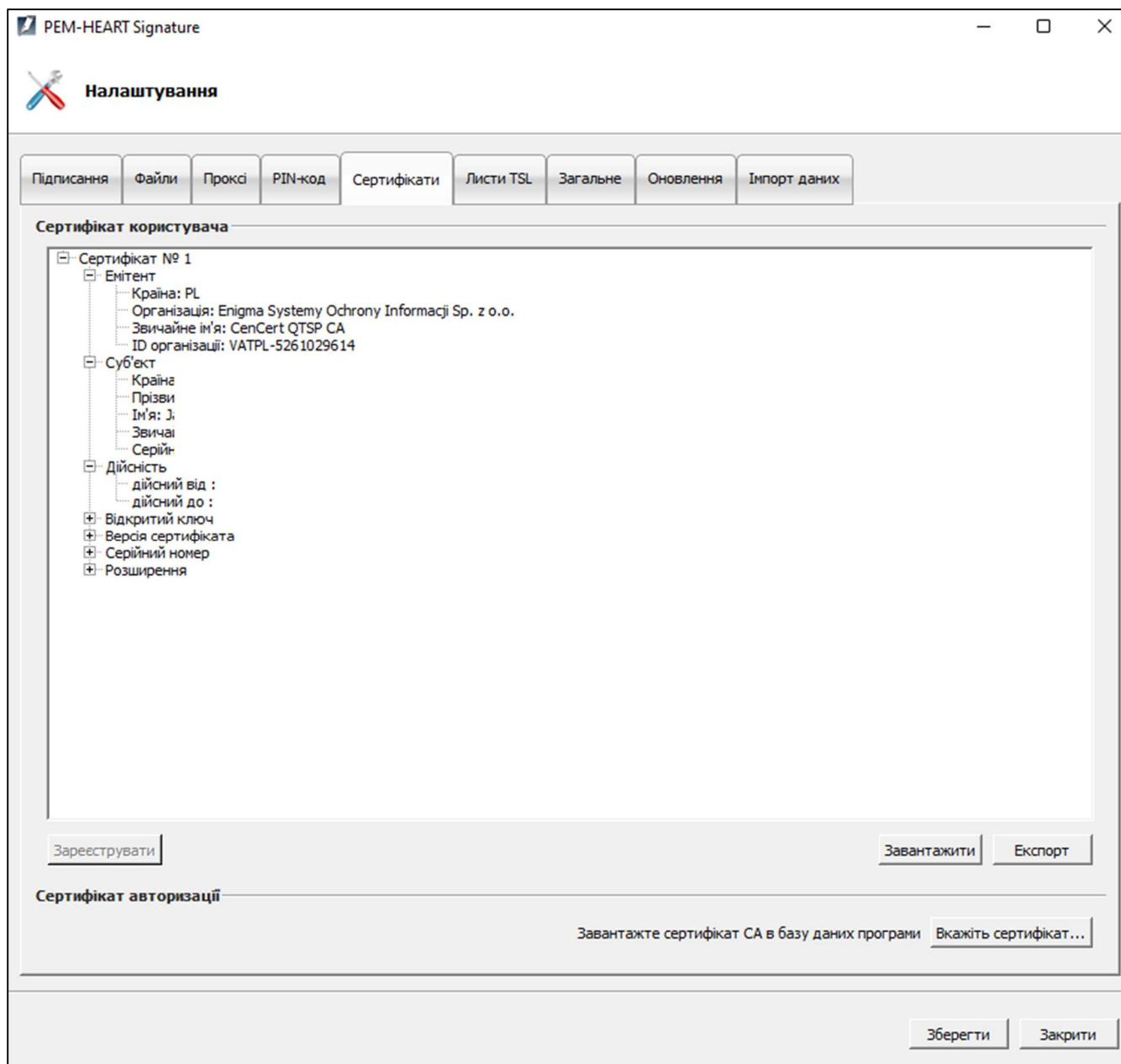
запам'ятовування програмою PIN-коду криптографічної картки.

Увага! Ця опція не застосовується до підписів rSign (у хмарі). Для цього типу підпису параметри налаштовуються в мобільному додатку.

За замовчуванням PIN-код запам'ятовується на час підписів для всіх документів у вікні підпису. Щоб підписати всі файли у вікні програми, вам потрібно лише один раз ввести PIN-код - після підписання повторний вибір файлів для підпису (навіть без закриття програми) означає, що вам потрібно буде ввести PIN-код ще раз. Також можна встановити інші параметри: щоб PIN-код завжди надавався для кожного окремого документа або щоб він зберігався в пам'яті комп'ютера протягом певного періоду часу.

8.5 СЕРТИФІКАТИ

Вкладка стосується представлення, реєстрації в системі та експорту сертифіката користувача. Якщо картку помістити в зчитувач, програма автоматично зчитує з неї дані, і вони відображаються у вікні. Якщо сертифікат не читається, перевірте розташування картки та скористайтеся кнопкою *Завантажити*. Якщо в системі встановлено токен rSign, він також буде показаний у списку після дії *Завантажити*.



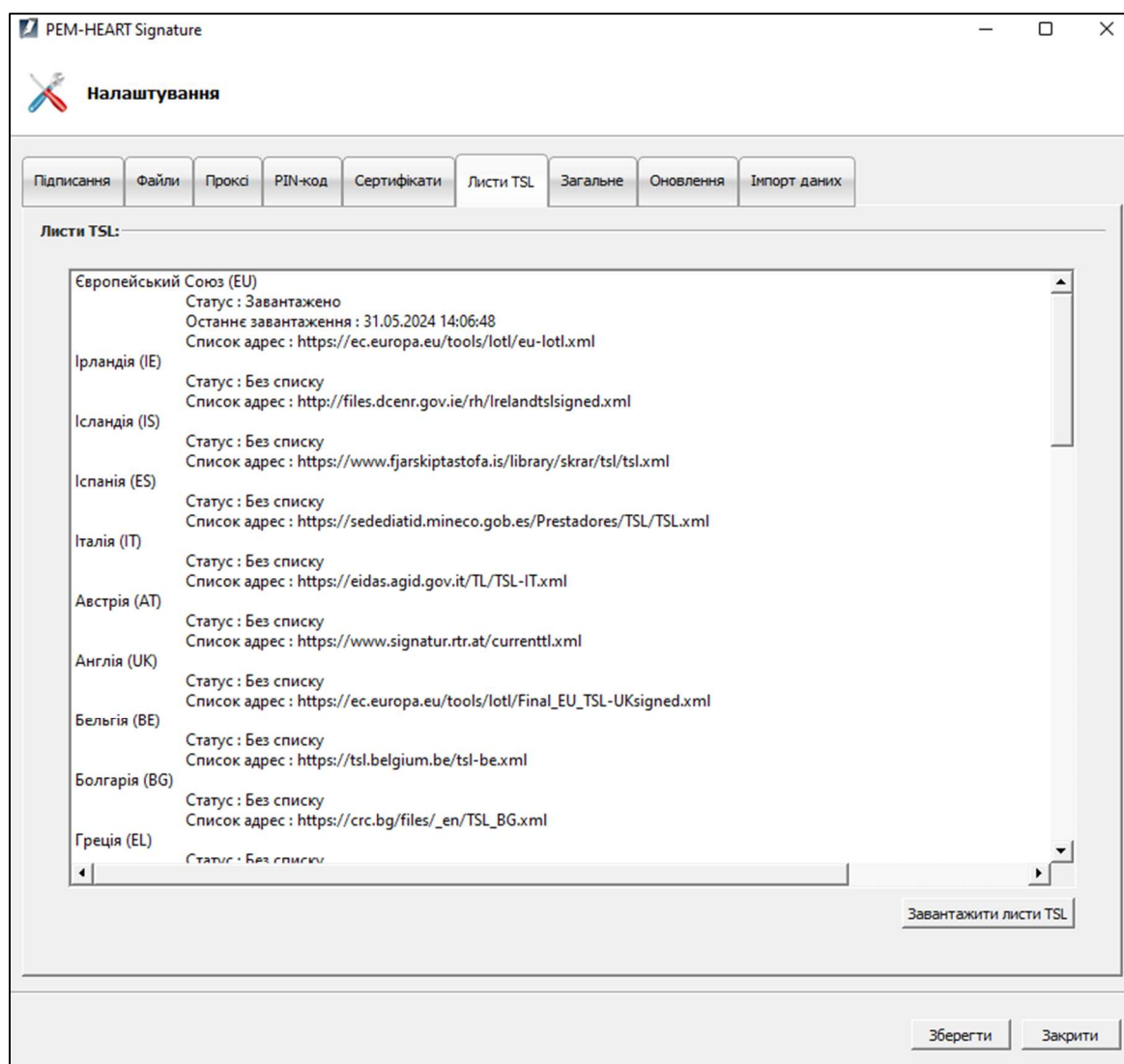
Мал. 57 Налаштування сертифіката користувача

Кнопка *Зареєструвати* використовується для реєстрації сертифіката, зчитаного з носія, у системному сховищі. Експортувати сертифікат у файл можна за допомогою кнопки *Експорт*. Розділ *Сертифікат центру* використовується для вказівки та завантаження такого сертифіката постачальника послуг довіри в базу даних програми. Опція використовується в конкретних ситуаціях щодо некваліфікованих підписів - коли програма не має в базі актуального сертифіката «проміжного органу» постачальника послуг довіри..

8.6 TSL СПИСКИ

Списки TSL містять усі необхідні дані про кваліфікованих постачальників довірчих послуг в ЄС (включно з польськими). Вони дозволяють перевіряти підписи, зроблені за допомогою кваліфікованих сертифікатів, виданих польськими та іншими постачальниками довірчих послуг ЄС.

Вкладка показує поточний стан списків TSL, доступних у програмі. Він також надає можливість ручного завантаження поточних списків TSL, виданих в окремих країнах (однак завантаження вручну не є обов'язковим для нормальної роботи, оскільки програма автоматично завантажує нові списки TSL, якщо під час перевірки підпису вона зустрічає сертифікат, який неможливо перевірити на основі сертифікатів, які



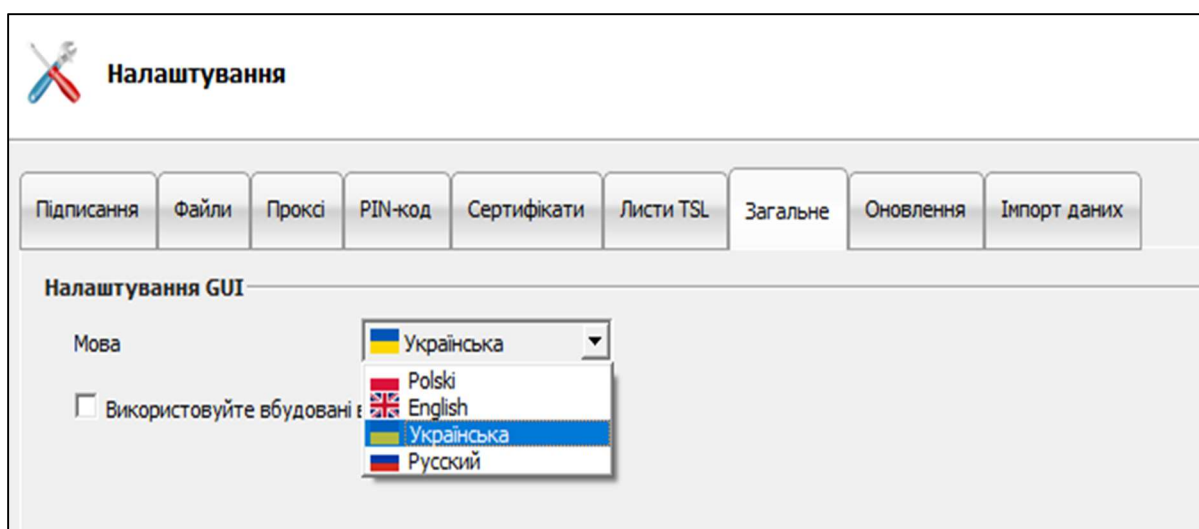
Мал. 58 Налаштування - списки TSL

має програма на даний момент у списку TSL). Щоб завантажити списки TSL, натисніть кнопку *Завантажити списки TSL*.

8.7 НАЛАШТУВАННЯ МОВИ

Змінити мову програми можна на вкладці «Загальні» на панелі «Налаштування». Мови на вибір: *польська, англійська, українська, російська*.

Параметр *Використовувати вбудовані вікна вибору файлів* використовується для зміни зовнішнього вигляду вікон, які з'являються під час вибору файлу, наприклад для підпису.



Мал. 59 Вибір мови, яка використовується в програмі

8.8 ОНОВЛЕННЯ

Версія програми відображається в головному вікні (правий нижній кут) PEM-HEART Signature. Крім того, у вкладці *Оновлення* можна перевірити, чи є нова версія. Інформацію про доступні оновлення можна надати вручну, натиснувши кнопку *Перевірити наявність оновлень*, або встановити параметри автоматичної перевірки під час запуску програми. Якщо буде виявлено нову версію програмного забезпечення, відобразяться повідомлення.



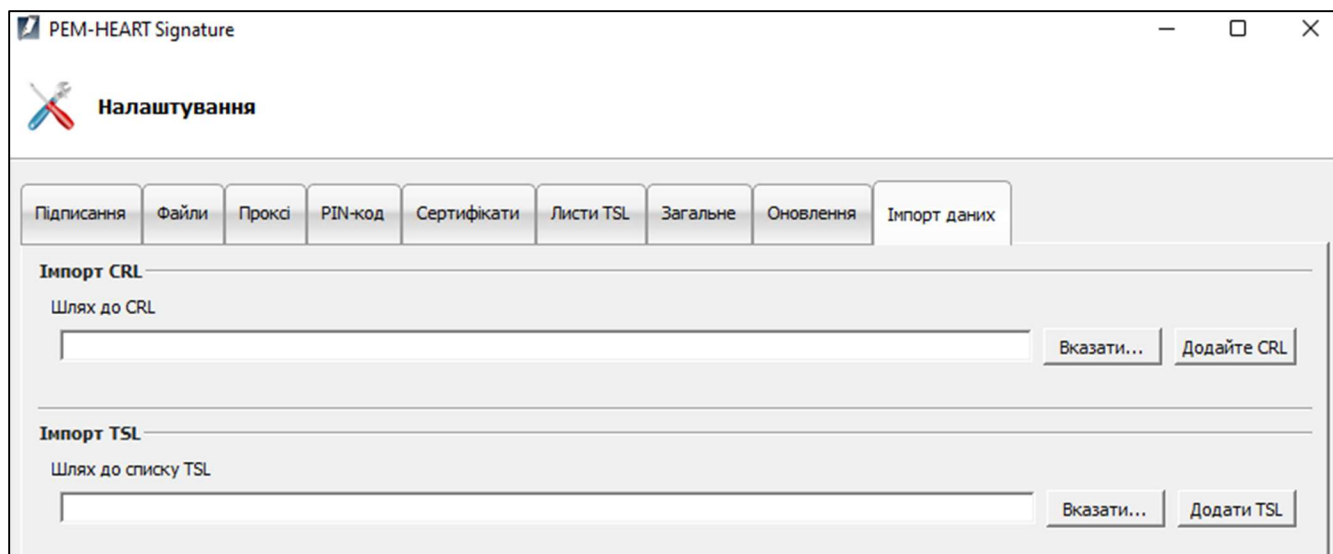
Мал. 60 Вікно з інформацією про версію програмного забезпечення

8.9 ІМПОРТ ДАНИХ

Параметри імпорту даних використовуються для того, щоб програма могла працювати в середовищі, де немає доступу до Інтернету. Додавання часових позначок і перевірка статусу сертифіката на основі OCSP у такій ситуації неможливі, але підпис і перевірка підпису все ще можливі, за умови, що програма має актуальні списки TSL і CRL, які в цьому випадку потрібно передати і завантажується в програму вручну.

Увага! Для створення підписів rSign (у хмарі) завжди потрібен доступ до Інтернету.

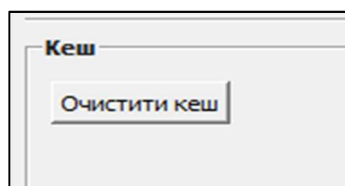
Щоб завантажити файл із CRL або TSL, натисніть кнопку *Вкажіть на відповідний список* (потім потрібно вибрати відповідний файл на диску), а потім кнопку *Додати CRL* або *Додати список TSL* відповідно.



Мал. 61 Параметри – імпорт даних списку CRL і TSL

8.9.1 ОЧИЩЕННЯ КЕШУ

Кнопка *Очистити кеш* видаляє базу даних програми *PEM-HEART Signature*. Це слід спробувати в окремих випадках, наприклад, коли виникає помилка бази даних. База даних містить дані кешу (наприклад, поточний список CRL), їх видалення не має жодних негативних наслідків, оскільки програма автоматично завантажить відсутні дані з мережевих ресурсів.



Мал. 62 Можливість очищення

9 ПІДПИС RSign

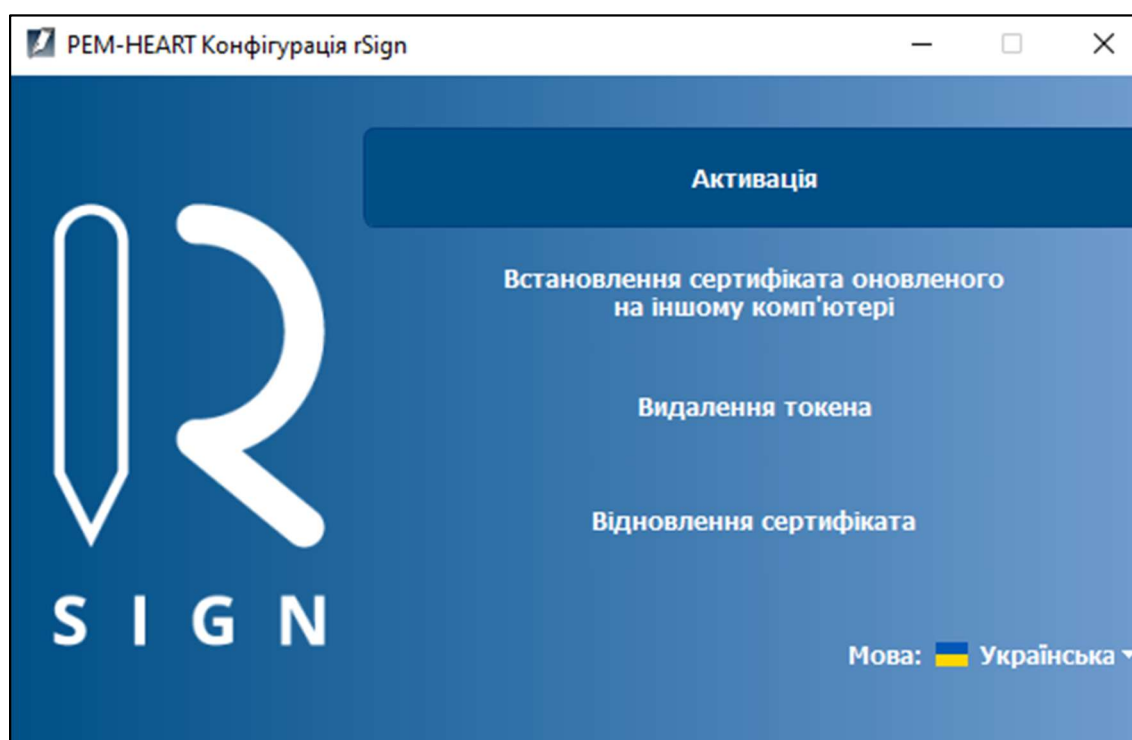
9.1 КОНФІГУРАЦІЯ НА КОМП'ЮТЕРІ

9.1.1 ДОДАВАННЯ ТОКЕНА RSign

Щоб використовувати rSign на певному комп'ютері (обліковий запис Windows), ви повинні налаштувати підпис на кожному такому комп'ютері (обліковому записі).

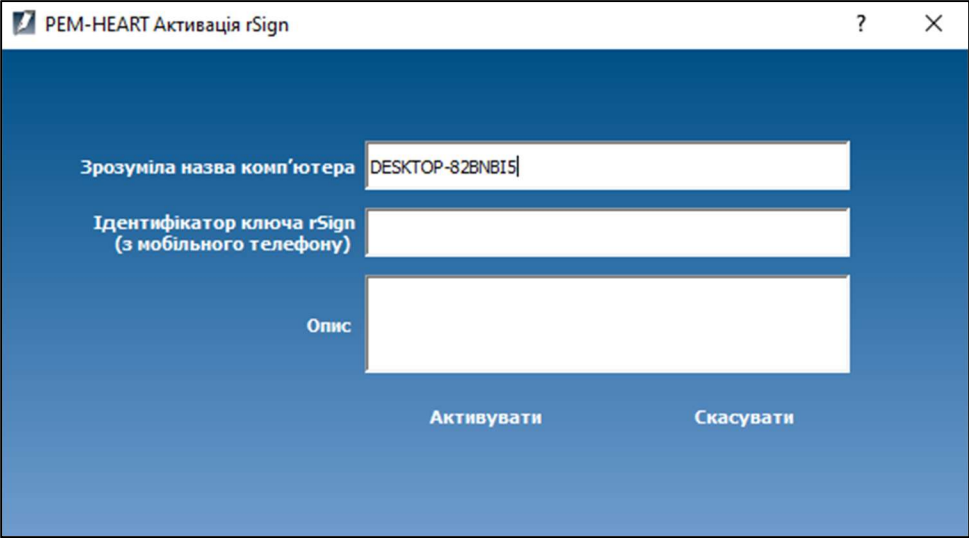
Цілі цієї операції подвійні - по-перше, починаючи створювати підпис, програма повинна знати, хто буде підписувати (яким сертифікатом буде підписаний підпис). По-друге, важливою метою є підвищення безпеки вашого підпису - rSign можна створити лише на комп'ютері, який ви раніше визнали надійним.

Щоб налаштувати підпис rSign, запустіть програму *PEM-HEART Signature* -> *Картка* -> *Налаштування rSign* або з меню Windows *PEM-HEART Налаштування rSign*. Потім натисніть кнопку *Активация*



Мал. 63 Конфігурація підпису rSign

Потім введіть Ідентифікатор ключа rSign із програми на своєму мобільному телефоні.



PEM-HEART Активация rSign

Зрозуміла назва комп'ютера DESKTOP-S2BNB15

Ідентифікатор ключа rSign
(з мобільного телефону)

Опис

Активувати Скасувати

Мал. 64 Вікно мобільного додатку з ідентифікатором ключа



14:45

←

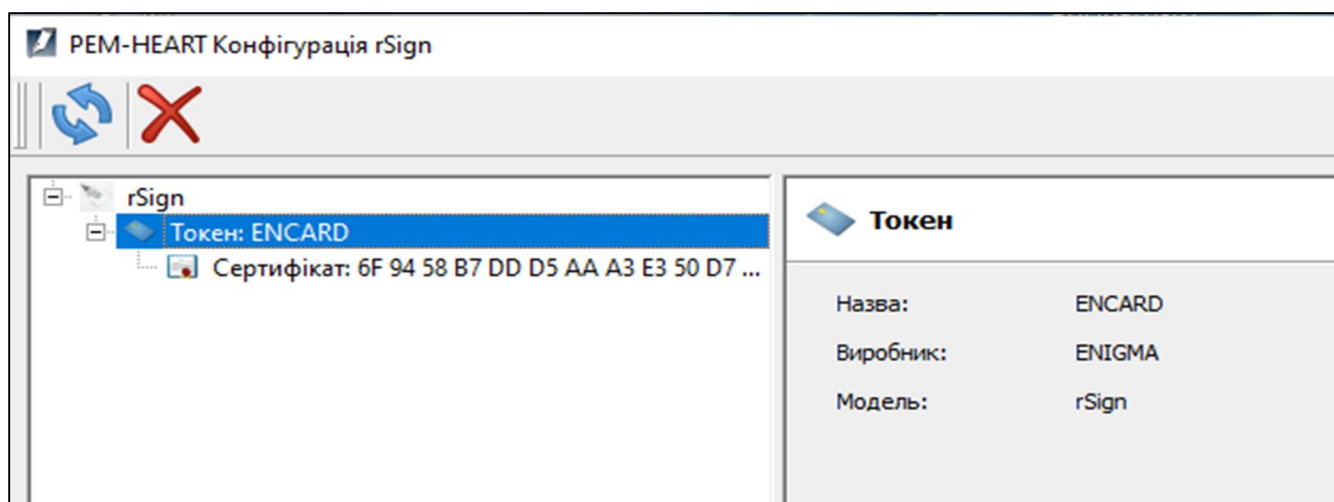
Ідентифікатор ключа

ЗАКРИТИ

Мал. 65 Вікно активації підпису

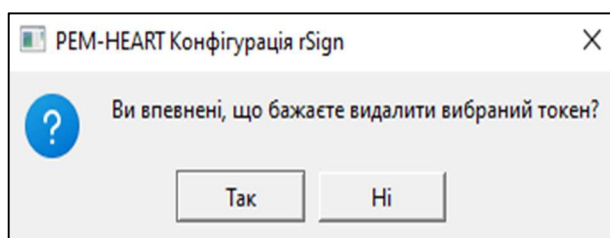
9.1.2 ВИДАЛЕННЯ ТОКЕНА RSign

Якщо є необхідність видалити токен rSign з комп'ютера, таку операцію можна виконати за допомогою програми *PEM-HEART Налаштування rSign*. Після запуску програми натисніть опцію *Видалення токenu*. Тоді буде відображено активний токен rSign в налаштуваннях та даних сертифіката.



Мал. 66 Перегляд активного токена rSign із даними сертифіката

Потім у вікні ліворуч натисніть *Токен: ENCARD*, який активує кнопку на  верхній панелі - її натискання запустить процес видалення токenu. Користувач повинен підтвердити видалення в окремому вікні:



Мал. 67 Підтвердження видалення токена rSign

Натиснувши *Так*, токен буде видалено.

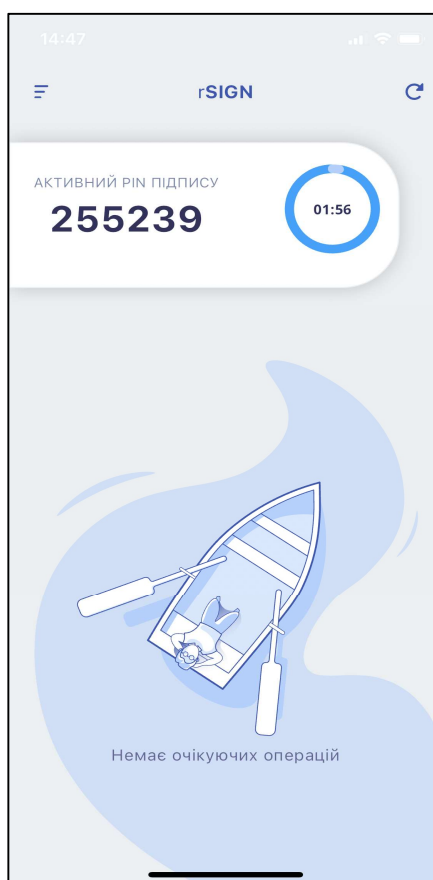
9.2 НАЛАШТУВАННЯ МОБІЛЬНОГО ДОДАТКУ

9.2.1 ВСТАНОВЛЕННЯ

Додаток доступний для завантаження в AppStore і Google Play.

9.2.2 ДОМАШНІЙ ЕКРАН

Після запуску програми за замовчуванням відображається екран із активним PIN-кодом підпису. У вікні Користувач бачить PIN-код, таймер із зазначенням часу його використання та чергу очікування операцій. Крім того, у верхньому правому куті є значок , використання якого оновлює перегляд сповіщень, і значок у верхньому лівому куті , після вибору якого, відобразяться параметри: *Операції*



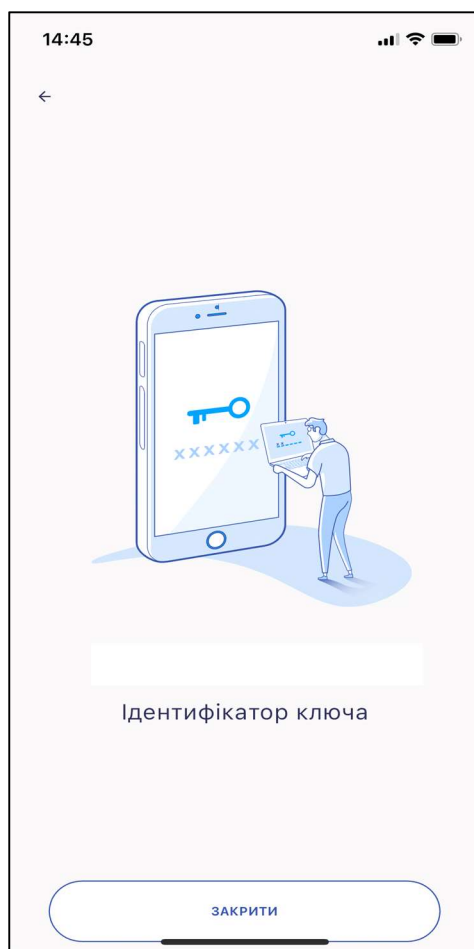
Мал. 68 Головний екран мобільного додатку rSign

(параметр за замовчуванням відображається під час запуску програми),
ідентифікатор ключа, налаштування.

9.2.3 ІДЕНТИФІКАТОР КЛЮЧА

Якщо вибрати ідентифікатор ключа, з'явиться екран із ідентифікатором ключа, який використовується

серед інших щоб налаштувати використання rSign на вашому комп'ютері. Однак, перш ніж користувач зможе його побачити, програма спочатку запитає PIN-код - лише якщо він введений правильно та підтверджено, ідентифікатор ключа буде відображено.



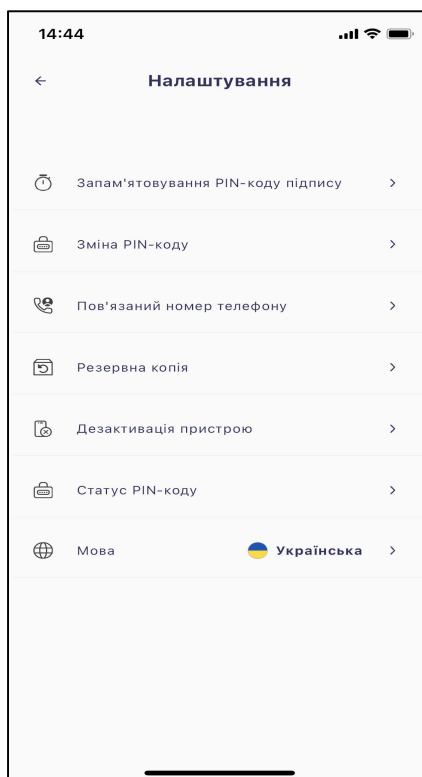
Мал. 69 Екран програми після вибору параметра Ідентифікатор ключа

9.2.4 НАЛАШТУВАННЯ

Якщо вибрати *Налаштування*, відобразиться екран зі списком доступних налаштувань програми. Це:

- *Запам'ятовування PIN-коду підпису* – опція, що дозволяє запам'ятати введений PIN-код на визначений Користувачем період часу. Доступні чотири варіанти - три попередньо визначені: 3, 5 і 10 хвилин і будь-який від 1 до 60 хвилин.
- *Зміна PIN-коду* – опція, яка дозволяє змінити PIN-код.
- *Пов'язаний номер телефону* – тут Користувач вводить номер телефону, пов'язаний з обліковим записом.
- *Резервне копіювання* – дозволяє створити резервну копію для активації rSign на будь-якому пристрої.
- *Деактивація пристрою* – опція, яка дозволяє видалити дані активації rSign з пристрою.

- *Мова* – дозволяє змінити мову в додатку. Мови на вибір: польська, англійська, російська, українська.



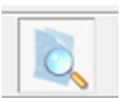
Мал. 70 Екран програми після вибору опції
Налаштування

10 АДМІНІСТРУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ PEM-HEART

10.1 ЖУРНАЛИ РОБОТИ КАРТОК ДЛЯ СИСТЕМ WINDOWS

Програмне забезпечення дозволяє увімкнути вхід для операцій, які виконуються за допомогою картки, наприклад, підписання документа. Увімкнути цю функцію можна двома способами:

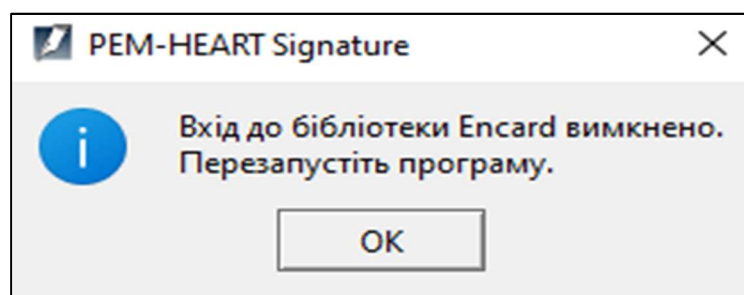
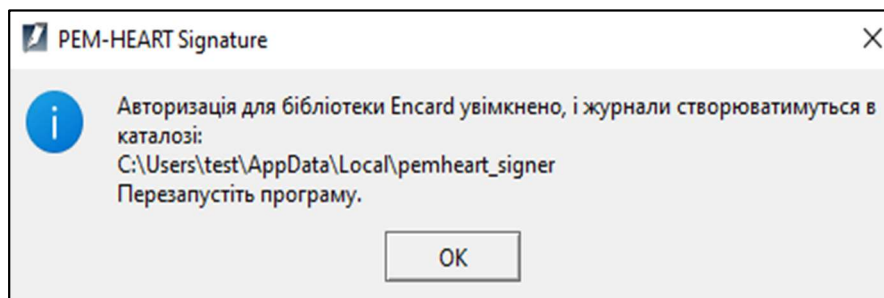
- Натиснувши значок «збільшувальне скло» на панелі Діагностика за допомогою розширених функцій.



- - іконка, що вказує на те, що функцію ввімкнено - при першому використанні перезапустить програму PEM-HEART Signature, щоб зберегти зміни,



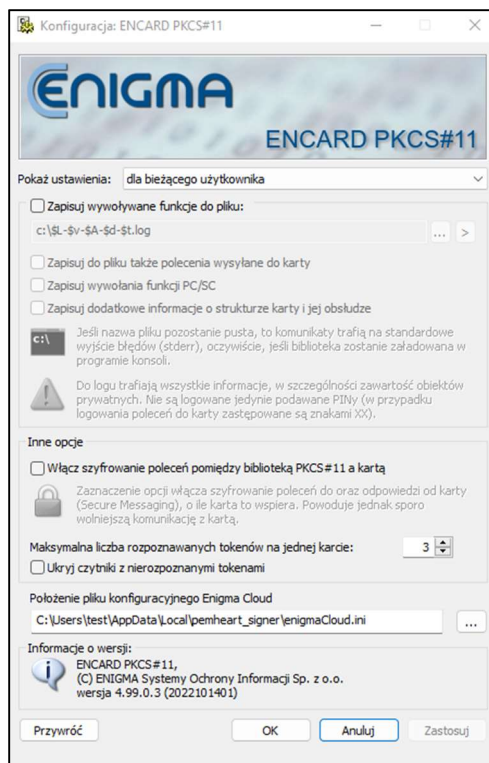
- іконка, яка вказує на те, що функція вимкнена - коли ви вмикаєте її вперше, вам потрібно перезапустити програму PEM-HEART Signature, щоб зберегти зміни.



Мал. 71 Повідомлення після ввімкнення та вимкнення входу в картки IDEMIA

- Більш розширена конфігурація викликається через вікна конфігурації бібліотеки PKCS#11. Виберіть *Меню«Пуск»->Програми->ENCARD->Налаштування* ENCARD PKCS#11. Вибір параметра конфігурації відкриє вікно для налаштування бібліотеки PKCS#11.

Вибір параметра Зберегти викликані функції у файл (це також назва першого розділу) використовується для налаштування запису всієї інформації до файлу журналу, зокрема вмісту приватних об'єктів. Введені PIN-коди не зберігаються - при вході в систему команди до картки замінюються символами XX.



Мал. 72 Екран конфігурації бібліотеки PKCS#11

Кнопка використовується для визначення розташування та імені файлу журналу. Якщо ім'я файлу залишити порожнім, повідомлення перейдуть до стандартної помилки (stderr), якщо бібліотеку завантажено в консольній програмі.

Бібліотека приймає спеціальні макроси в назві файлу, які дозволяють записувати в різні файли журналу залежно від програми, яка його завантажує, поточного часу та дати, версії бібліотеки тощо. Натискання кнопки  поруч із назвою файлу журналу відображається діалогове вікно конфігурації зі списком усіх макросів:

- \$A - ім'я файлу програми, яка завантажує бібліотеку (без шляху та розширення).
- \$L - ім'я файлу завантаженої бібліотеки (без шляху та розширення).
- \$I - внутрішня назва бібліотеки.
- \$D - дата завантаження бібліотеки у вигляді YYYY-MM-DD.
- \$d - дата завантаження бібліотеки у вигляді YYYYMMDD.
- \$T - час завантаження бібліотеки у вигляді hh-mm-ss.
- \$t - час завантаження бібліотеки у вигляді hhmmss.

- \$K - номер збірки бібліотеки (nr. 2008080901).
- \$V - основна версія бібліотеки (nr. 2.0).
- \$v - повна версія бібліотеки (nr. 2.01.2.2).
- \$\$ - знак \$.

Зберігаючи викликані функції у файл, користувач може вибрати іншу інформацію, щоб додати до журналу додаткову інформацію. Додаткові параметри включають:

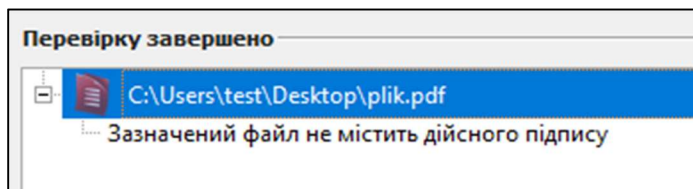
- *Також зберігати у файл команди, надіслані на карту*
- *Реєстрація викликів функцій PC/SC*
- *Записати додаткову інформацію про структуру картки та її функціонування*

У другому розділі вікна конфігурації бібліотеки PKCS#11 можна додати шифрування до з'єднання між бібліотекою PKCS#11 і картою, встановивши прапорець Увімкнути шифрування команд між бібліотекою PKCS#11 і картою. Крім того, ви можете вказати максимальну кількість розпізнаних токенів на одній картці та приховати зчитувачі з нерозпізнаними токенами.

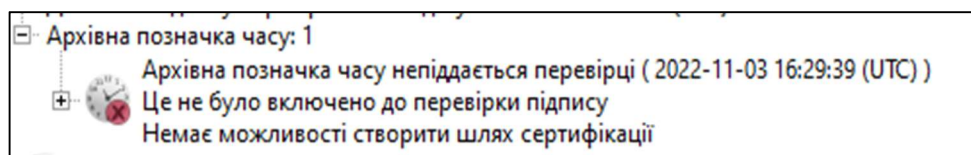
Відразу під другим розділом є місце для вказівки шляху до конфігураційного файлу Enigma Cloud та інформації про програмне забезпечення конфігурації.

Усі зміни зберігаються натисканням кнопки *Застосувати*. Вибір *ОК* також зберігає зміни та закриває відкрите вікно конфігурації. Будь-які зміни параметрів можна скасувати, вибравши *Скасувати* (закриття вікна конфігурації без збереження змін) або *Відновити* (відновлення налаштувань з моменту відразу після запуску конфігуратора, без закриття програми).

11 ВИРІШЕННЯ ПРОБЛЕМ



Мал. 73 Повідомлення про відсутність дійсного



Мал. 74 Повідомлення про позначку часу архіву, що не підлягає перевірці

МОНТАЖ		
Проблема	Причина	Рішення
Операція не вдалася	Користувач скасував процес встановлення програми	Перезапустіть інсталятор

ПІДПИСАННЯ		
Проблема	Причина	Рішення
Позначку часу не вдалося отримати з жодного із серверів	Із сертифікатом не пов'язано жодного пакета часових позначок	- спробуйте ще раз наступного дня або - придбати пакет позначення часу (деталі: http://www.cencert.pl), або - вимкнути часові позначки підписів (див. Розділ 6.2 Позначення часу)
	Програма не має доступу до Інтернету або запит не був	- перевірте підключення до Інтернету - перевірте налаштування

	схвалений у додатку rSign	проксі (якщо Ви використовуєте проксі-сервер) - див. Розділ 8.3 Проксі)
Функціональність недоступна для поточного носія !!!	Немає реалізованої функції для підтримки перевірки даного файлу, підпис зроблено в непідтримуваному стандарті	Заява в Cencert

ПЕРЕВІРКА		
Проблема	Причина	Рішення
Вказати місцезнаходження документів. Не всі відключені документи знайдено...	Програма не знайшла підписаний файл у каталозі підписів.	Вказати файл, який підписаний (відповідає підпису, який перевіряється)
Помилка відкриття вхідного файлу	Файл пошкоджено або відкрито в іншій програмі	Закрийте іншу програму, а потім спробуйте знову відкрити файл у PEM-HEART Signature.
	Файл уже відкрито в іншій програмі	
	Програма не має доступу до розташування файлу	Перевірте, чи дійсно файл існує у вказаному місці
Жоден із файлів не містить дійсного підпису	Файл пошкоджено або підписаний у форматі, який не підтримується PEM-HEART Signature	Вказування іншого файлу або звітування в Cencert

12 СПИСОК МАЛЮНКІВ

Мал. 1 Вікно запуску майстра встановлення	9
Мал. 2 Вікно майстра встановлення	10
Мал. 3 Вікно, що завершує роботу майстра встановлення	10
Мал. 4 Встановлення Thales SafeNet.....	11
Мал. 5 Вікно для завершення процесу встановлення.....	11
Мал. 6 Можливості модифікації встановлення	12
Мал. 7 Видалення програми	12
Мал. 8 Підтвердження видалення програми.....	13
Мал. 9 Пакет PemHeart для macOS	14
Мал. 10 Встановлювач пакетів Pem-Heart - вікно запуску	15
Мал. 11 Встановлювач пакетів Pem-Heart - ліцензійна угода	16
Мал. 12 Встановлювач пакетів Pem-Heart - прийняття ліцензійної угоди.....	16
Мал. 13 Встановлювач пакетів Pem-Heart - інформація про встановлення	17
Мал. 14 Встановлювач пакетів Pem-Heart - підсумок встановлення	18
Мал. 15 Встановлювач пакетів SafeNet Authentication Client - вікно запуску	19
Мал. 16 Встановлювач пакетів SafeNet Authentication Client – ліцензійна угода	20
Мал. 17 Встановлювач пакетів SafeNet Authentication Client - прийняття ліцензійної угоди	21
Мал. 18 Встановлювач пакетів SafeNet Authentication Client – інформація про встановлення.....	22
Мал. 19 Встановлювач пакетів SafeNet Authentication Client - підсумок встановлення	23
Мал. 20 Повідомлення про видалення додатку Pem-Heart із запитом на видалення.....	24
Мал. 21 Повідомлення про видалення із запитом на видалення конфігурації Pem-Heart	24
Мал. 22 Повідомлення про видалення із запитом на видалення конфігурації rSign.....	25
Мал. 23 Підтвердження видалення програми.....	25

Мал. 24 Програма видалення SafeNet Authentication Client – вікно запуску	26
Мал. 25 Програма видалення SafeNet Authentication Client – підсумок видалення	27
Мал. 26 Встановлення програми для Linux через файловий менеджер	28
Мал. 27 Програма видалення програми для Linux через файловий менеджер	30
Мал. 28 Приклад функцій PPM для файлу PDF	31
Мал. 29 Вікно з атрибутами підпису	36
Мал. 30 Вікно з деталями сертифіката	37
Мал. 31 Статус підпису після перевірки	38
Мал. 32 Головне меню програми PEM-HEART Signature - вибір опції «Підписати»	40
Мал. 33 Вікно подачі електронного підпису	41
Мал. 34 Повідомлення щодо користування додатком rSign на телефоні	42
Мал. 35 Екран додатку rSign із активним PIN-кодом для підпису	43
Мал. 36 Погодження на виконання операції електронного підпису	44
Мал. 37 Вікно для введення PIN-коду та підтвердження операції підпису (телефон)	45
Мал. 38 Підтвердження операції підпису (комп'ютер)	46
Мал. 39 Головне меню програми PEM-HEART Signature - вибір опції «Перевірити»	47
Мал. 40 Вікно перевірки електронного підпису	48
Мал. 41 Головне меню програми PEM-HEART Signature - розширені функції	49
Мал. 42 Вікно подання контрпідпису	50
Мал. 43 Вікно для нанесення позначки часу на електронний підпис	51
Мал. 44 Підписання XML-документа з вкладеннями - перехід до налаштування розташування підпису	53
Мал. 45 Головне меню програми PEM-HEART Signature - вибір вкладки «Картка»	55
Мал. 46 Зразок екрана програми для карти Thales типу A	56
Мал. 47 Зразок екрана програми для IDEMIA Encard	57

Мал. 48 Екран зміни PIN-коду картки IDEMIA	58
Мал. 49 Розблокування карти - вибір токена - картка IDPrime	59
Мал. 50 Додаткові параметри на екрані Діагностики	60
Мал. 51 Вигляд відкритої панелі Діагностики - відображення токена з картки та rSign	61
Мал. 52 Вікно для зміни параметрів підпису	63
Мал. 53 Визначення вихідних каталогів для оброблених документів	65
Мал. 54 Проксі-сервер - налаштування системи	65
Мал. 55 Проксі-сервер - налаштування вручну	66
Мал. 56 Налаштування ПІН-коду	67
Мал. 57 Налаштування сертифіката користувача	68
Мал. 58 Налаштування - списки TSL	69
Мал. 59 Вибір мови, яка використовується в програмі	70
Мал. 60 Вікно з інформацією про версію програмного забезпечення	71
Мал. 61 Параметри – імпорт даних списку CRL і TSL	72
Мал. 62 Можливість очищення	72
Мал. 63 Конфігурація підпису rSign	73
Мал. 64 Вікно мобільного додатку з ідентифікатором ключа	74
Мал. 65 Вікно активації підпису	74
Мал. 66 Перегляд активного токена rSign із даними сертифіката	75
Мал. 67 Підтвердження видалення токена rSign	75
Мал. 68 Головний екран мобільного додатку rSign	76
Мал. 69 Екран програми після вибору параметра Ідентифікатор ключа	77
Мал. 70 Екран програми після вибору опції Налаштування	79
Мал. 71 Повідомлення після ввімкнення та вимкнення входу в картки IDEMIA	81
Мал. 72 Екран конфігурації бібліотеки PKCS#11	82

Мал. 73 Повідомлення про відсутність дійсного	84
Мал. 74 Повідомлення про позначку часу архіву, що не підлягає перевірці.....	84