

КЛЮЧ ЕЛЕКТРОННИЙ DIAMOND
УТИЛІТА НАЛАШТУВАННЯ ТА КЕРУВАННЯ (ГРАФІЧНА)
НАСТАНОВА КОРИСТУВАЧА

Версія 8.6.1

ЗМІСТ

1. ЗАГАЛЬНІ ВІДОМОСТІ	3
1.1 Атестат ключа	3
2. СИСТЕМНІ ВИМОГИ	4
3. ВСТАНОВЛЕННЯ ТА ЗАПУСК	4
3.1 Особливості роботи у Windows.....	4
3.2 Особливості роботи в Linux	5
3.3 Особливості роботи в macOS	6
4. ГОЛОВНЕ ВІКНО	6
5. ОБЛІКОВІ ЗАПИСИ KE DIAMOND	7
6. РОЛЬ КОРИСТУВАЧА	8
6.1 Зміна пароля	9
6.2 Генерація ключів	10
6.3 Імпорт.....	12
6.3.1 Імпорт ключів з файлу PKCS#12	12
6.3.2 Імпорт сертифіката.....	13
6.3.3 Імпорт даних	13
6.4 Експорт	14
6.5 Запит на сертифікат	14
6.6 Властивості.....	15
6.7 Видалити.....	15
6.8 Оновити	15
6.9 Вийти	16
7. РОЛЬ АДМІНІСТРАТОРА БЕЗПЕКИ	16
7.1 Зміна пароля	17
7.2 Ініціалізація KE	17
7.3 Параметри безпеки	18
7.4 Розблокування	18
7.5 Журнал подій	19
7.6 Вийти	19
8. МОЖЛИВІ ПРОБЛЕМИ	19

1. ЗАГАЛЬНІ ВІДОМОСТІ

Програмний засіб «KE DIAMOND. Утиліта налаштування та керування» (далі – Утиліта) призначено для роботи з ключами електронними DIAMOND (далі – KE). Утиліта дозволяє:

- отримувати відомості про KE: модель, заводський номер, версію мікропрограми, кількість спроб входу та результат самотестування;
- змінювати паролі Користувача та Адміністратора безпеки;
- розблоковувати обліковий запис Користувача та встановлювати кількість невдалих спроб автентифікації до його блокування;
- ініціалізувати KE – встановлювати новий пароль Користувача зі знищенням усіх ключів, сертифікатів і даних Користувача;
- генерувати ключі ДСТУ 4145, ECDSA та RSA і одразу формувати запити на сертифікати відкритих ключів, зокрема з атестатами ключів;
- імпортувати на KE ключі з файлів PKCS#12 (PFX), сертифікати відкритих ключів та довільні дані;
- експортувати з KE сертифікати й дані, копіювати ключі на інший KE (за умови, що експорт дозволений при генерації);
- формувати запити на сертифікати для ключів, що вже зберігаються на KE;
- переглядати властивості об'єктів, змінювати їхні назви та ідентифікатори, видаляти об'єкти;
- переглядати журнал аудиту KE.

1.1 Атестат ключа

Атестат ключа – підтвердження, яке формує сам KE щодо ключа, що на ньому зберігається. Атестат засвідчує, що особистий ключ згенеровано всередині KE і що вивести його з KE неможливо (ключ неекспортуємий).

Атестат призначено для кваліфікованого надавача електронних довірчих послуг (центру сертифікації ключів). Перш ніж видати кваліфікований сертифікат відкритого ключа, надавач має переконатися, що відповідний особистий ключ згенерований та зберігається в засобі кваліфікованого електронного підпису без можливості експорту. Атестат, вкладений у запит на сертифікат (некритичне розширення запиту), дає таке підтвердження без пред'явлення самого KE: надавач перевіряє атестат і те, що ідентифікатор ключа в атестаті відповідає відкритому ключу в запиті. Разом з атестатом до запиту додається ідентифікатор та заводський номер носія – KE DIAMOND.

2. СИСТЕМНІ ВИМОГИ

Утиліта працює в таких 64-розрядних операційних системах:

- Microsoft Windows 10 (версія 1607 і новіші), Windows 11, Windows Server 2016 і новіші на платформі x86-64;
- macOS 12 (Monterey) і новіші на комп'ютерах з процесорами Intel (x86-64) та Apple Silicon (arm64);
- Linux на платформі x86-64 з бібліотекою glibc версії 2.17 і новішою (Debian, Ubuntu, Fedora, Red Hat Enterprise Linux, Oracle Linux 7 і новіші тощо) з графічним середовищем X11 або Wayland, службою pcsd та драйвером CCID – пакетом libccid (Debian, Ubuntu та ін.) або pcsc-lite-ccid (Fedora, Red Hat та ін.) версії 1.4.31 і новішої.

Утиліта працює з KE DIAMOND моделей 1000, 2000 і старших. Набір доступних функцій залежить від моделі та версії мікропрограми KE:

- алгоритм RSA – на моделях 2000 і старших;
- кнопка підтвердження (сенсорна кнопка «присутності») – на моделях 3000 і старших;
- атестати ключів – на KE з мікропрограмою 7 і новішою;
- зміна назви та ідентифікатора ключа – на KE з мікропрограмою 8.5 і новішою.

Для підключення KE потрібен вільний порт USB.

Монітор з роздільною здатністю не меншою за 1024×768 .

3. ВСТАНОВЛЕННЯ ТА ЗАПУСК

Утиліта не потребує встановлення: вона постачається одним файлом (для macOS – пакетом програми), який достатньо скопіювати на комп'ютер і запустити.

KE працює через стандартний драйвер смарт-карток CCID та службу PC/SC операційної системи, окремі драйвери не потрібні. Користувач, який запускає Утиліту, повинен мати доступ до пристроїв зчитування смарт-карток.

Якщо до комп'ютера підключено кілька KE, потрібний обирається в полі «Ключ електронний» головного вікна (рис. 1). KE, підключений після запуску Утиліти, з'являється в переліку після натискання кнопки «Оновити перелік».

3.1 Особливості роботи у Windows

- Файл Утиліти – `diamond-util-gui.exe`, запуск – подвійним кліком.

- KE визначається вбудованим драйвером Windows як «Microsoft Usbccid Smartcard Reader (WUDF)». Має працювати служба «Смарт-картка» (Smart Card, SCardSvr) – зазвичай вона запускається автоматично під час підключення KE.
- Під час запуску файлу, завантаженого з Інтернету, фільтр SmartScreen може показати попередження. У такому разі натисніть «Додаткові відомості», а потім «Виконати все одно».
- У сеансі віддаленого робочого столу (RDP) Утиліта бачить лише KE, підключені до комп'ютера, з якого встановлено з'єднання, і лише якщо в параметрах підключення дозволено перенаправлення смарт-карток. KE, підключені безпосередньо до віддаленого комп'ютера, у сеансі RDP недоступні.

3.2 Особливості роботи в Linux

- Має бути встановлено та запущено службу pcsd і драйвер CCID. Debian, Ubuntu:

```
sudo apt install pcsd libccid
```

- Fedora, Red Hat Enterprise Linux, Oracle Linux (у версії 7 – yum замість dnf):

```
sudo dnf install pcsc-lite pcsc-lite-ccid
```

- Запуск служби:

```
sudo systemctl enable --now pcsd.socket
```

(у системах без активації через сокет – pcsd.service).

- Утиліта постачається архівом diamond-util-gui-linux-x64.tar.gz або файлом AppImage.
- Архів розпакуйте в будь-яку теку. Запуск – з термінала командою ./start.sh або ./diamond-util-gui, чи подвійним кліком на ярлику diamond-util-gui.desktop у файловому менеджері. Перед першим запуском ярлик треба дозволити: контекстне меню ярлика → «Дозволити запуск». Сам файл diamond-util-gui подвійним кліком не запускається: файлові менеджери (зокрема GNOME Files) не розпізнають його як програму.
- Файл AppImage: дозвольте його виконання (властивості файлу або команда `chmod +x`) і запустіть подвійним кліком. Для роботи AppImage потрібна бібліотека FUSE 2 – пакет libfuse2 (Ubuntu 22.04 і новіші) або fuse-libs (Fedora, Red Hat). Без FUSE файл AppImage запускається з термінала з параметром --appimage-extract-and-run.

- У дистрибутивах, де доступ до pcsd контролює polkit, KE доступний лише з локального графічного сеансу користувача; з віддаленого сеансу (SSH, XRDP) доступ може бути заборонено.

3.3 Особливості роботи в macOS

- Утиліта постачається образом диска «KE DIAMOND.dmg». Відкрийте його подвійним кліком і перетягніть «KE DIAMOND.app» у теку «Програми». Запуск – з Launchpad або теки «Програми».
- Пакет універсальний: він працює на комп'ютерах і з процесорами Intel, і з Apple Silicon.
- KE працює через вбудований у macOS драйвер CCID, додаткові драйвери не потрібні.

4. ГОЛОВНЕ ВІКНО

Після запуску Утиліти відкривається головне вікно (рис. 1), у якому відображаються основні відомості про обраний KE.

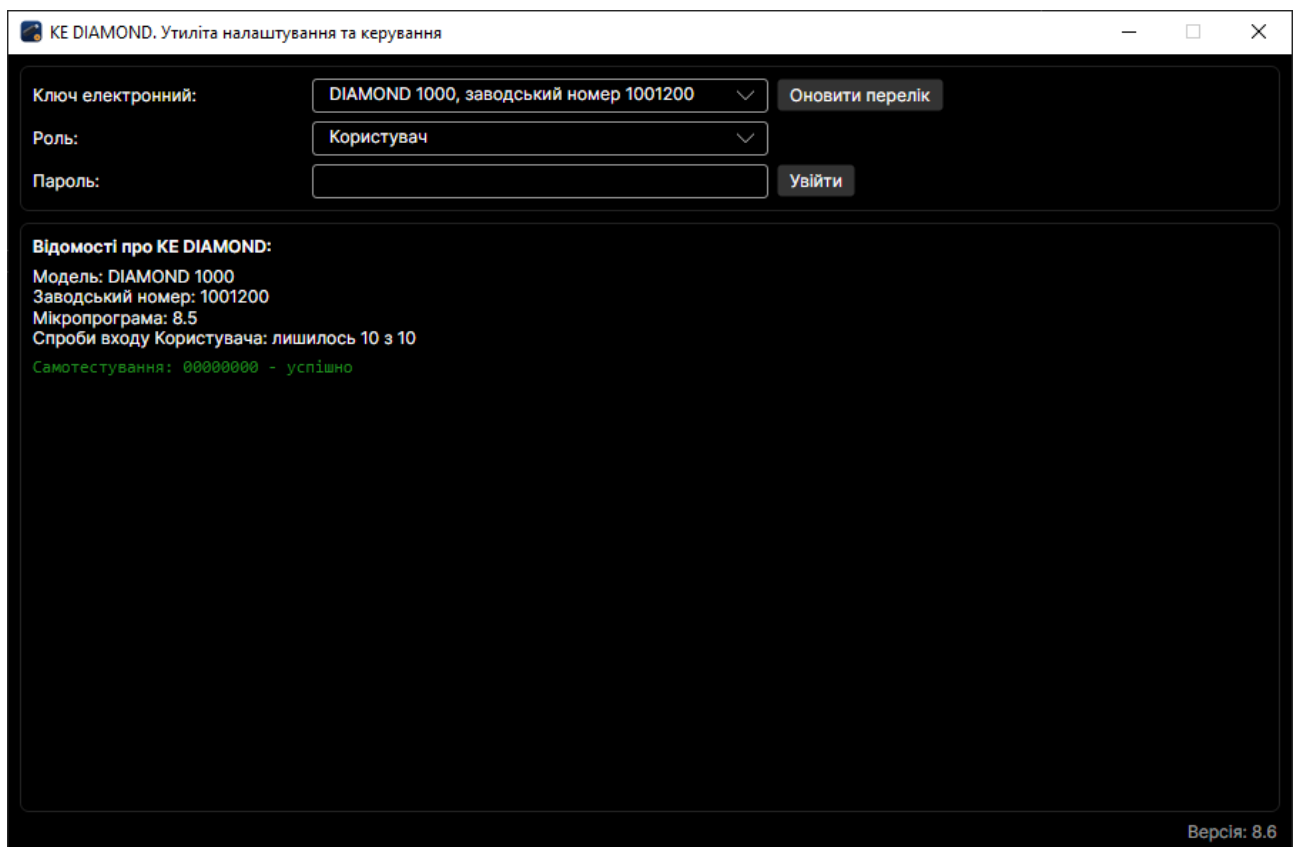


Рисунок 1 – Головне вікно Утиліти

У верхній частині головного вікна розташовані:

- «Ключ електронний» – вибір KE з переліку підключених;
- кнопка «Оновити перелік» – повторний пошук підключених KE;

- «Роль» – вибір облікового запису: «Користувач» або «Адміністратор безпеки»;
- «Пароль» – поле введення пароля обраної ролі та кнопка «Увійти».

У полі «Відомості про KE DIAMOND» відображаються:

- модель KE;
- заводський номер KE;
- версія мікропрограми KE;
- кількість спроб входу Користувача, що лишилися, та їх загальна кількість;
- результат самотестування KE (зеленим кольором – успішне, червоним – помилка).

У нижньому рядку вікна відображається результат останньої операції або повідомлення про помилку, праворуч – версія Утиліти.

5. ОБЛІКОВІ ЗАПИСИ KE DIAMOND

У KE DIAMOND є два облікові записи (далі – ролі) з різними можливостями: Користувач та Адміністратор безпеки.

Кількість невдалих спроб автентифікації Користувача обмежується апаратно. Після введення правильного пароля лічильник невдалих спроб автентифікації Користувача скидається в 0. Кількість невдалих спроб автентифікації Адміністратора безпеки не обмежується, тому Адміністратор безпеки має використовувати достатньо стійкий пароль.

Пароль може містити від 4 до 64 символів.

Заводські налаштування:

- пароль Адміністратора безпеки – 000000;
- пароль Користувача – 111111;
- кількість невдалих спроб автентифікації до блокування облікового запису Користувача – 10.

Увага! Заводські паролі Адміністратора безпеки та Користувача мають бути змінені до початку використання KE DIAMOND!

Увага! У разі втрати пароля Адміністратора безпеки використання KE DIAMOND буде обмежене, а в разі втрати паролів і Адміністратора безпеки, і Користувача використання KE DIAMOND за призначенням буде неможливим. Зберігайте пароль Адміністратора безпеки у спосіб, що виключає його втрату та компрометацію!

6. РОЛЬ КОРИСТУВАЧА

Для входу в роль Користувача в головному вікні оберіть роль «Користувач», введіть пароль Користувача в поле «Пароль» і натисніть клавішу Enter або кнопку «Увійти». Після входу відображається перелік об'єктів, що зберігаються на KE (рис. 2).

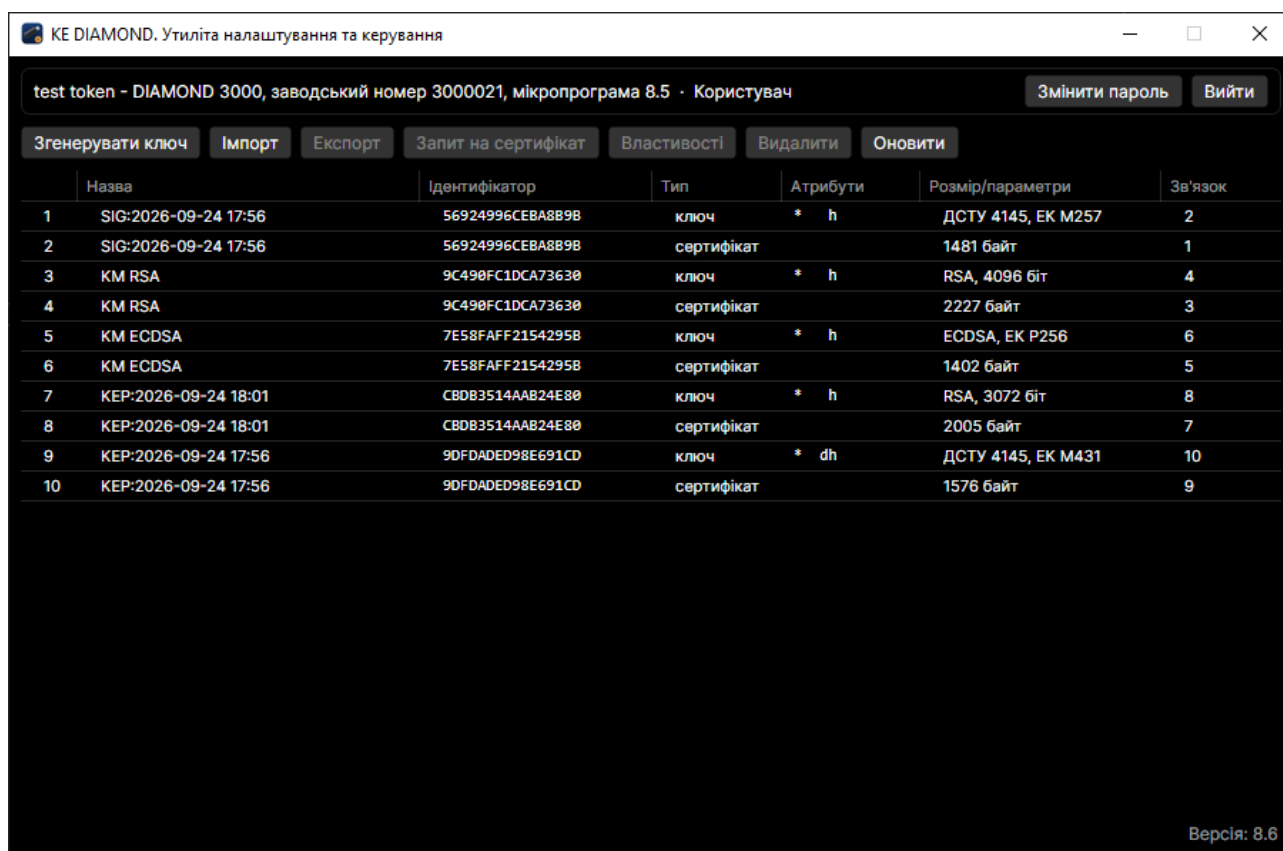


Рисунок 2 – Вікно Утиліти в ролі Користувача

Обліковий запис Користувача використовується для повсякденної роботи:

- генерації, використання та знищення особистих і таємних ключів;
- створення атестатів особистих ключів (п. 1.1);
- запису, зчитування та знищення сертифікатів відкритих ключів і довільних даних;
- зміни власного пароля.

У верхньому рядку вікна відображаються назва KE, його модель, заводський номер, версія мікропрограми та поточна роль, а також кнопки «Змінити пароль» і «Вийти». Нижче розташовані кнопки операцій з об'єктами та таблиця об'єктів з такими колонками:

- перша колонка – порядковий номер рядка;
- «Назва» – назва (мітка, label) об'єкта;

- «Ідентифікатор» – ідентифікатор (id) об'єкта: ключ і його сертифікати мають однаковий ідентифікатор;
- «Тип» – ключ, сертифікат або дані;
- «Атрибути» – позначки властивостей об'єкта (табл. 1);
- «Розмір/параметри» – алгоритм і параметри ключа або розмір сертифіката чи даних;
- «Зв'язок» – номери рядків пов'язаних об'єктів: для ключа – його сертифікатів, для сертифіката – його ключа.

Таблиця 1 – Позначки в колонці «Атрибути»

Позначка	Значення
*	приватний об'єкт: доступний лише після входу на KE (без позначки – доступний без автентифікації)
e	експортуємий ключ: його можна скопіювати на інший KE (п. 6.4)
d	ключ узгодження ключів (шифрування, ECDH)
h	ключ згенеровано пристроєм (без позначки – ключ імпортовано)
b	для операцій з ключем потрібна кнопка підтвердження (моделі 3000 і старші)
s	для кожної операції з ключем потрібне окреме натискання кнопки (разом з позначкою b)

Подвійний клік на рядку таблиці відкриває вікно властивостей об'єкта (п. 6.6). Кнопки операцій, недоступних для обраного об'єкта, неактивні; підказка біля такої кнопки пояснює причину.

6.1 Зміна пароля

Для зміни пароля Користувача натисніть кнопку «Змінити пароль». У діалоговому вікні (рис. 3) введіть новий пароль у поля «Новий пароль» і «Підтвердження пароля» та натисніть клавішу Enter або кнопку «Змінити». Для скасування натисніть клавішу Esc або кнопку «Скасувати».

Рисунок 3 – Зміна пароля Користувача

Увага! У разі втрати пароля Користувача використання KE DIAMOND буде обмежене: продовжити роботу можна лише після ініціалізації KE

Адміністратором безпеки (п. 7.2), яка знищує всі ключі, сертифікати та дані Користувача.

6.2 Генерація ключів

Для генерації ключів натисніть кнопку «Згенерувати ключ». У діалоговому вікні (рис. 4) оберіть параметри генерації та натисніть клавішу Enter або кнопку «Згенерувати». Для скасування натисніть клавішу Esc або кнопку «Скасувати».

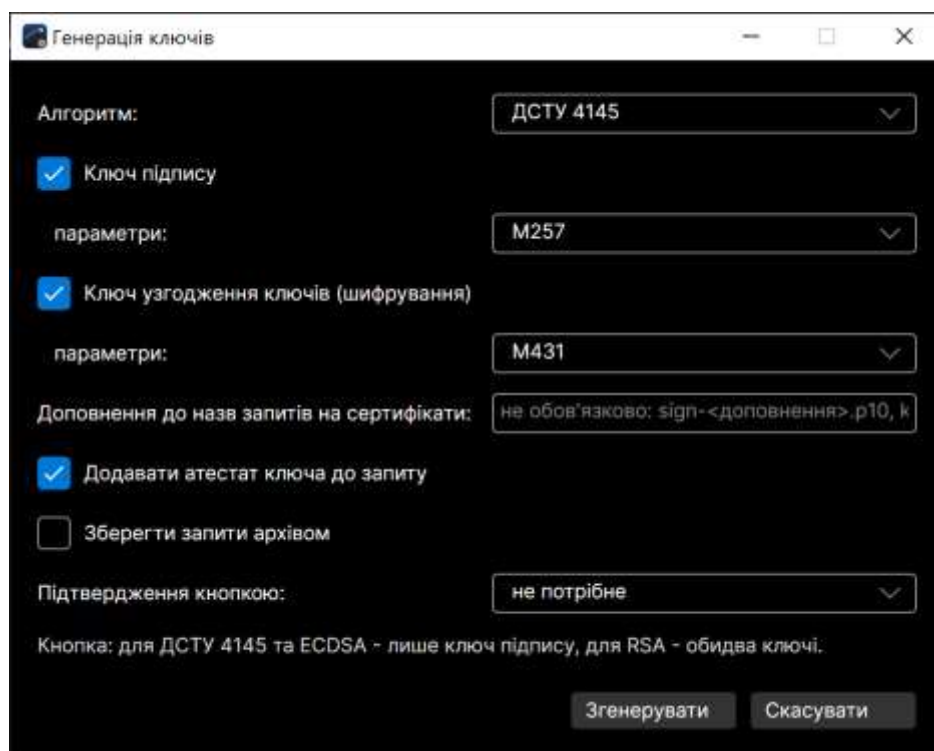


Рисунок 4 – Генерація ключів

Параметри генерації ключів наведено в табл. 2. Алгоритми та параметри, які обраний KE не підтримує, неактивні.

Таблиця 2 – Параметри генерації ключів

Параметр	Значення
Алгоритм	ДСТУ 4145, ECDSA або RSA (RSA – на моделях 2000 і старших)
Ключ підпису	генерувати ключ для накладання електронного підпису
параметри (ключа підпису)	еліптична крива для ДСТУ 4145: M257 (типово), M233, M307, M367, M431; для ECDSA: P-256 (типово), P-384, P-521; довжина ключа RSA: 2048 (типово), 3072, 4096 біт
Ключ узгодження ключів (шифрування) (для RSA – Ключ шифрування ключів)	генерувати ключ для узгодження ключів шифрування (для RSA – для шифрування ключів)
параметри (ключа узгодження)	як для ключа підпису; для ДСТУ 4145 типово – M431

Параметр	Значення
Доповнення до назв запитів на сертифікати	необов'язковий текст, що додається до назв файлів запитів: sign-<доповнення>.p10 і кер-<доповнення>.p10; без доповнення – sign.p10 і кер.p10
Додавати атестат ключа до запиту	включити до запиту на сертифікат атестат ключа (п. 1.1); типово увімкнено, неактивне, якщо KE не підтримує атестати
Зберегти запити архівом	зберегти запити одним архівом ZIP замість окремих файлів
Підтвердження кнопкою	режим кнопки підтвердження (табл. 3); лише на моделях 3000 і старших

Можна генерувати обидва ключі одночасно або лише один з них; хоча б один ключ має бути обраний.

Таблиця 3 – Режими кнопки підтвердження

Режим	Значення
не потрібне	ключ використовується без натискання кнопки
кнопку натиснуто під час підпису	операція виконується, лише поки кнопку утримують натиснутою; доки кнопку не відпущено, можна виконати будь-яку кількість операцій
окреме натискання для кожного підпису	кожне натискання дозволяє виконати рівно одну операцію; для наступної кнопки треба відпустити й натиснути знову

Для ДСТУ 4145 та ECDSA кнопка захищає лише ключ підпису, для RSA – обидва ключі, оскільки шифрування ключів RSA виконується тією самою операцією з особистим ключем, що й підпис. Режим кнопки задається лише під час створення ключа і надалі не змінюється.

Назви ключам Утиліта присвоює автоматично: «SIG:» – для ключа підпису, «KER:» – для ключа узгодження (шифрування) ключів, далі – дата й час натискання кнопки «Згенерувати» за всесвітнім координованим часом (UTC), наприклад «SIG:2026-10-05 07:15». Обидва ключі пари отримують однаковий час, тож за назвами видно, що ключі парні. Якщо ключ з такою назвою вже є (генерація повторюється протягом тієї самої хвилини), до назви додаються секунди. Назву можна змінити згодом у вікні властивостей (п. 6.6).

Після генерації Утиліта для кожного ключа формує запит на сертифікат відкритого ключа (формат PKCS#10) і пропонує обрати теку для збереження запитів (або файл архіву). Запит містить відкритий ключ і його ідентифікатор; відомості про власника (subject) у запиті не заповнюються – їх вносить кваліфікований надавач електронних довірчих послуг під час видачі сертифіката. Якщо від збереження запитів відмовитися, їх можна сформулювати пізніше кнопкою «Запит на сертифікат» (п. 6.5).

Генерація ключів RSA може тривати до кількох хвилин. Якщо ключ підпису потребує кнопки, для підписання запиту Утиліта попросить натиснути кнопку на KE та чекатиме до 30 секунд.

6.3 Імпорт

Для запису на KE об'єкта з файлу натисніть кнопку «Імпорт» і оберіть файл. Тип вмісту файлу Утиліта визначає автоматично, незалежно від розширення:

- файл ключів PKCS#12 (PFX, P12) – імпортуються ключі та їхні сертифікати (п. 6.3.1);
- сертифікат відкритого ключа X.509 у форматі DER або PEM – імпортується сертифікат (п. 6.3.2);
- будь-який інший файл – записується як дані Користувача (п. 6.3.3).

6.3.1 Імпорт ключів з файлу PKCS#12

Імпорт ключів виконується у два кроки. Спочатку відкривається вікно «Файл ключів <ім'я файлу>», у якому потрібно ввести пароль до файлу і натиснути кнопку «Відкрити». Якщо у файлі немає особистих ключів, Утиліта повідомляє про це, і імпорт завершується.

Далі відкривається вікно «Імпорт ключів з <ім'я файлу>». У його верхній частині вказано кількість ключів і сертифікатів у файлі та алгоритм, яким захищено файл. Для кожного ключа відображаються:

- прапорець «Імпортувати ключ <алгоритм і параметри>, сертифікатів: N» – вмикає або вимикає імпорт цього ключа (типово увімкнено);
- «Назва» – назва ключа на KE (до 32 байтів). Типово це назва ключа з файлу (friendlyName), а якщо її немає – «SIG:» або «KER:» з датою та часом відкриття файлу за UTC, як і в згенерованих ключів (п. 6.2). Однакові назви ключів з одного файлу Утиліта розрізняє, додаючи порядковий номер;
- «Для узгодження ключів (шифрування)» – лише для ключів на еліптичних кривих: ключ призначено для узгодження ключів шифрування (ECDH). Типове значення визначається за сертифікатом ключа (використання ключа – keyUsage), якщо сертифіката немає – за назвою з префіксом «KER:»; якщо у файлі два ключі ДСТУ 4145 без жодних підказок, другий вважається ключем узгодження.

Ключі, які KE не підтримує, показуються з позначкою «пропускається» і не імпортуються. Спільні параметри імпорту:

- «Підтвердження кнопкою» – режим кнопки (табл. 3), лише на моделях 3000 і старших;
- «Сертифікати доступні без автентифікації» – сертифікати з файлу можна буде читати без входу на КЕ (типово увімкнено).

Перед імпортом Утиліта перевіряє, що обрано хоча б один ключ, назви не порожні, не довші за 32 байти, різні і що на КЕ ще немає ключів з такими назвами. Для імпорту натисніть клавішу Enter або кнопку «Імпортувати», для скасування – клавішу Esc або кнопку «Скасувати». Після імпорту в нижньому рядку вікна відображається кількість імпортованих ключів і сертифікатів, а також причини, з яких щось не записано.

Разом з ключами записуються їхні сертифікати з того самого файлу. Імпортовані ключі не експортуються: скопіювати їх на інший КЕ неможливо. Імпортований ключ не має позначки «згенеровано пристроєм» (h), тому атестат для нього не формується, а запит на сертифікат формується без атестата.

6.3.2 Імпорт сертифіката

Сертифікат записується на КЕ лише тоді, коли на КЕ вже є особистий ключ цього сертифіката: Утиліта шукає ключ, відкритий ключ якого збігається з відкритим ключем у сертифікаті. Якщо такого ключа немає, сертифікат не імпортується, і Утиліта повідомляє: «На носії немає особистого ключа цього сертифіката. Сертифікат без свого ключа не записується». Сертифікат, який на КЕ вже є, повторно не записується.

Назву та ідентифікатор сертифікат отримує від свого ключа, тому в таблиці об'єктів ключ і сертифікат пов'язані (колонка «Зв'язок»). У діалоговому вікні імпорту відображаються власник сертифіката та назва його ключа; параметр «Доступ без автентифікації» дозволяє читати сертифікат без входу на КЕ.

6.3.3 Імпорт даних

Будь-який інший файл записується як дані Користувача (рис. 5). У діалоговому вікні вкажіть:

- «Назва об'єкта» – типowo ім'я файлу без розширення;
- «Назва додатку» – необов'язкова назва програми, якій належать дані;
- «Доступ без автентифікації» – дозволити читання даних без входу на КЕ.

Для завершення натисніть клавішу Enter або кнопку «Імпортувати», для скасування – клавішу Esc або кнопку «Скасувати».

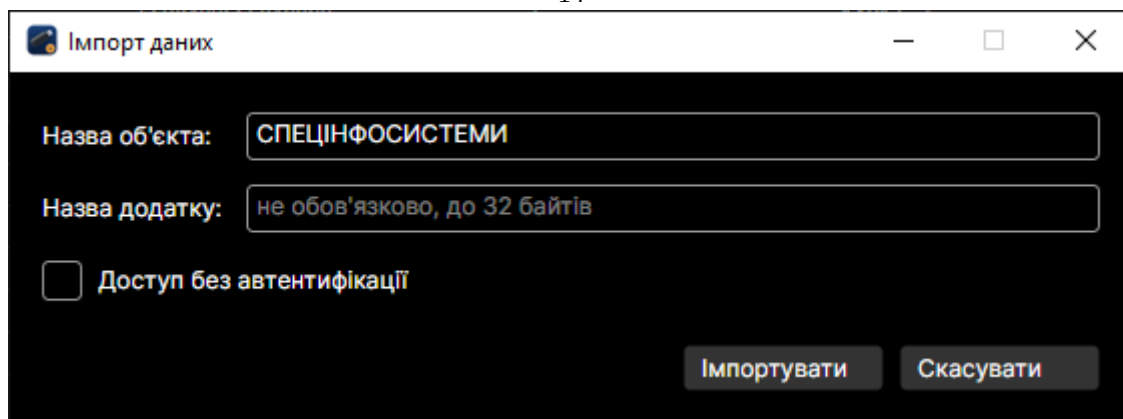


Рисунок 5 – Імпорт даних

Назви об'єктів і додатків обмежено 32 байтами в кодуванні UTF-8: літера латиниці займає 1 байт, літера кирилиці – 2 байти, тобто назва може містити не більше 16 літер кирилиці.

6.4 Експорт

Для експорту оберіть об'єкт у таблиці та натисніть кнопку «Експорт»:

- сертифікат зберігається у файл формату DER (розширення .cer);
- дані Користувача зберігаються у файл (розширення .bin);
- ключ експортується лише для копіювання на KE DIAMOND і лише за наявності позначки «експортуємий» (e). Особистий ключ у файл не зберігається. Ключі, згенеровані або імпортовані Утилітою, цієї позначки не мають; вона може бути лише в ключів, створених іншими програмами.

Під час експорту ключа відкривається вікно «Копіювання ключа на KE». У ньому оберіть KE призначення (це може бути й той самий KE), для іншого KE введіть пароль його Користувача, вкажіть нову назву ключа та параметри: «Ключ можна експортувати», «Дозволено узгодження ключів» і «Підтвердження кнопкою» (табл. 3; доступне, якщо KE призначення має кнопку). Обидва KE мають бути підключені до комп'ютера.

6.5 Запит на сертифікат

Для формування запиту на сертифікат для ключа, що вже є на KE, оберіть ключ у таблиці, натисніть кнопку «Запит на сертифікат» і вкажіть файл для збереження (типово – назва ключа з розширенням .p10). Для ключа, згенерованого KE, до запиту автоматично додається атестат ключа (п. 1.1); для імпортованого ключа запит формується без атестата. Якщо ключ потребує кнопки, натисніть кнопку на KE, коли Утиліта про це попросить (протягом 30 секунд).

6.6 Властивості

Для перегляду властивостей об'єкта оберіть його та натисніть кнопку «Властивості» або двічі клацніть рядок таблиці (рис. 6). Відображаються тип об'єкта, алгоритм або розмір, розшифровка атрибутів, ідентифікатор ключа, пов'язані сертифікати чи ключ, а для сертифіката – його власник, видавець, строк чинності та серійний номер.

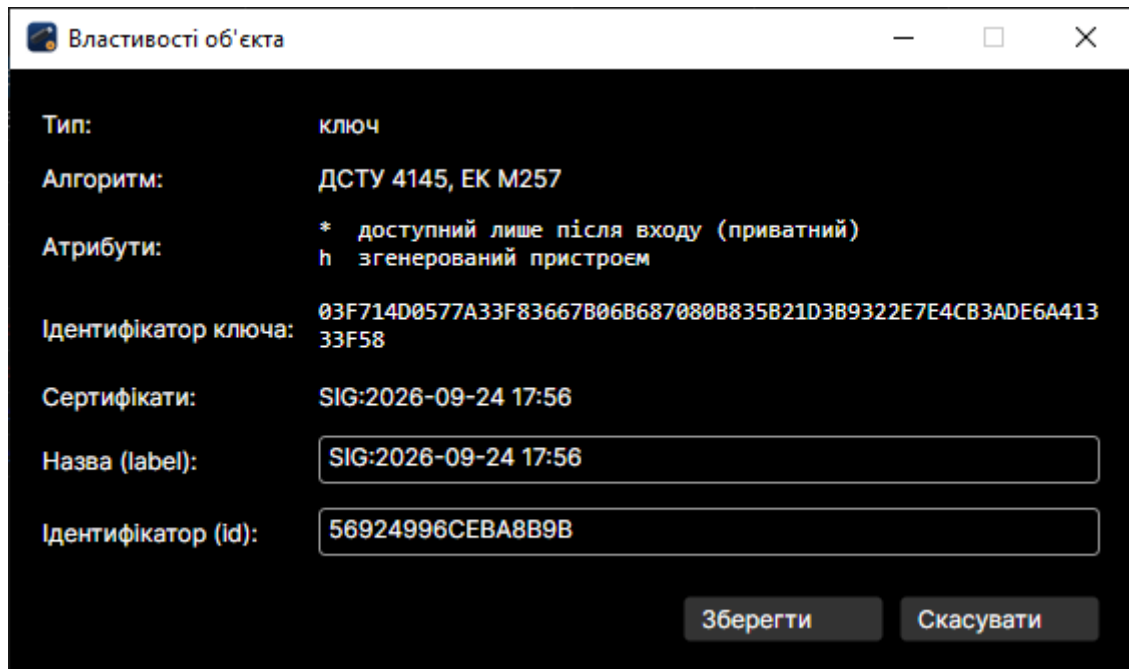


Рисунок 6 – Властивості об'єкта

У полях «Назва (label)» та «Ідентифікатор (id)» можна змінити назву (до 32 байтів) та ідентифікатор (шістнадцятковий рядок, до 32 байтів) об'єкта і зберегти зміни кнопкою «Зберегти». Змінювати назву та ідентифікатор ключа дозволяє мікропрограма 8.5 і новіша, якщо Адміністратор безпеки не заборонив це (п. 7.3).

6.7 Видалити

Для видалення оберіть об'єкт і натисніть кнопку «Видалити», у вікні підтвердження – кнопку «Видалити» або клавішу Enter; для скасування – кнопку «Скасувати» або клавішу Esc. Разом із ключем видаляються всі його сертифікати. Якщо видаляється єдиний сертифікат ключа, Утиліта запропонує видалити також і ключ.

Увага! Видалений ключ відновити неможливо.

6.8 Оновити

Для оновлення переліку об'єктів на КЕ натисніть кнопку «Оновити».

6.9 Вийти

Для завершення роботи в ролі Користувача та повернення до головного вікна натисніть кнопку «Вийти».

7. РОЛЬ АДМІНІСТРАТОРА БЕЗПЕКИ

Для входу в роль Адміністратора безпеки в головному вікні оберіть роль «Адміністратор безпеки», введіть пароль Адміністратора безпеки в поле «Пароль» і натисніть клавішу Enter або кнопку «Увійти» (рис. 7).

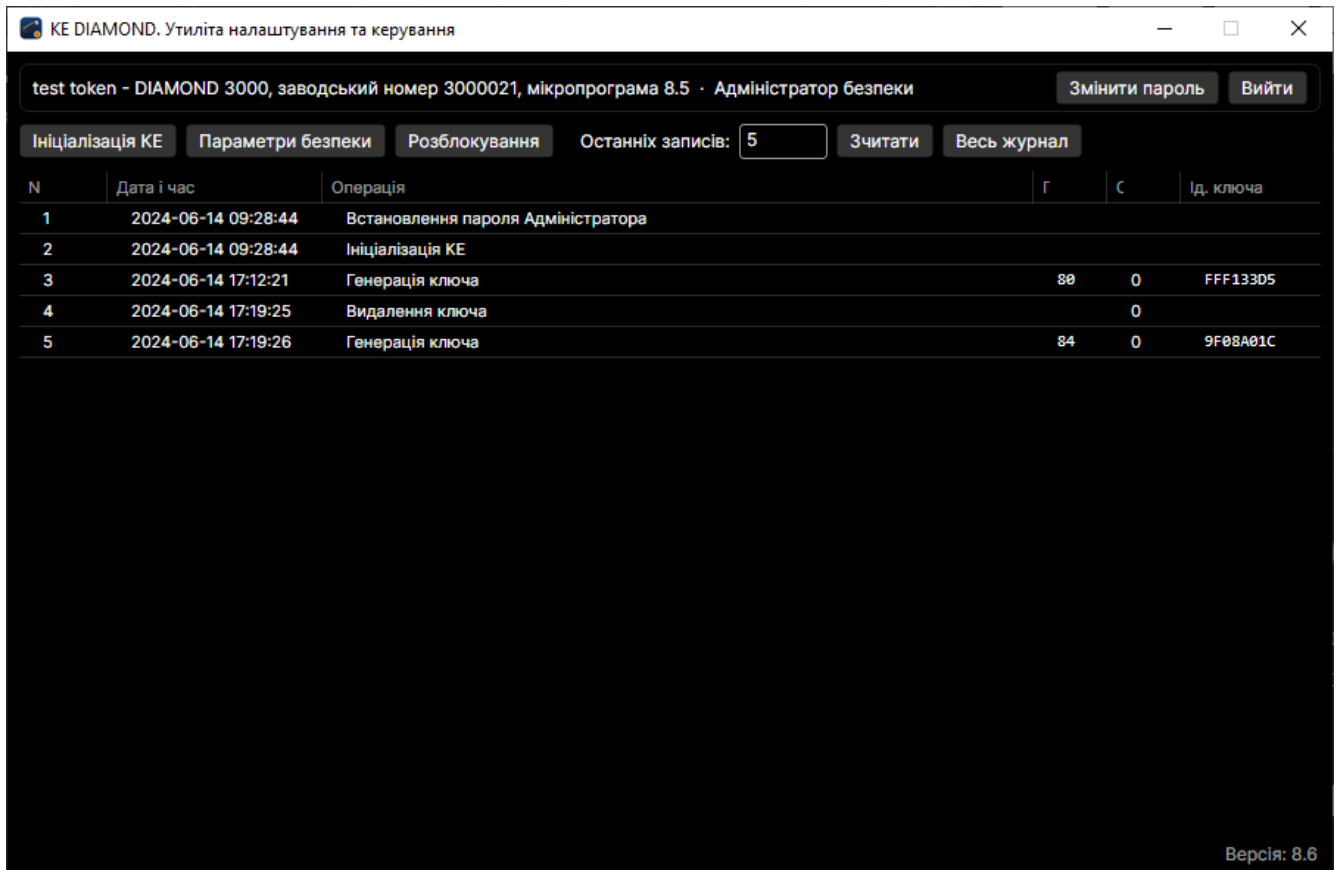


Рисунок 7 – Вікно Утиліти в ролі Адміністратора безпеки

Обліковий запис Адміністратора безпеки використовується для:

- встановлення кількості невдалих спроб автентифікації Користувача до блокування його облікового запису (від 1 до 100);
- розблокування облікового запису Користувача;
- встановлення нового пароля Користувача зі знищенням усіх ключів, сертифікатів і даних Користувача;
- зміни власного пароля;
- перегляду журналу подій.

7.1 Зміна пароля

Для зміни пароля Адміністратора безпеки натисніть кнопку «Змінити пароль». У діалоговому вікні (рис. 8) введіть новий пароль у поля «Новий пароль» і «Підтвердження пароля» та натисніть клавішу Enter або кнопку «Змінити». Для скасування натисніть клавішу Esc або кнопку «Скасувати».

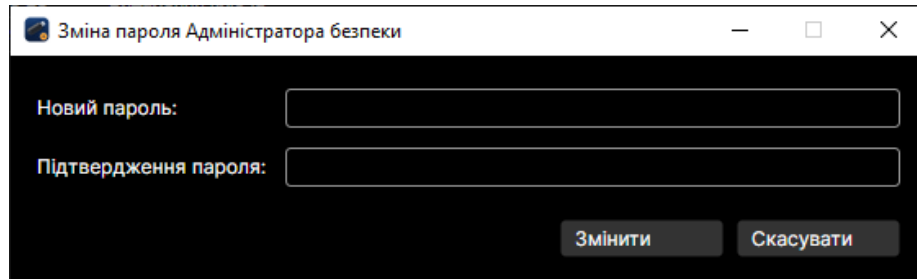


Рисунок 8 – Зміна пароля Адміністратора безпеки

Увага! У разі втрати паролів і Користувача, і Адміністратора безпеки використання KE DIAMOND за призначенням буде неможливим. Зберігайте пароль Адміністратора безпеки у спосіб, що виключає його втрату та компрометацію!

7.2 Ініціалізація KE

Для встановлення нового пароля Користувача зі знищенням усіх ключів, сертифікатів і даних Користувача натисніть кнопку «Ініціалізація KE». У діалоговому вікні (рис. 9) введіть новий пароль Користувача в поля «Новий пароль Користувача» і «Підтвердження пароля», за потреби вкажіть назву KE в полі «Назва KE (label)» (до 32 байтів, можна лишити порожньою) і натисніть клавішу Enter або кнопку «Форматувати». Для скасування натисніть клавішу Esc або кнопку «Скасувати».

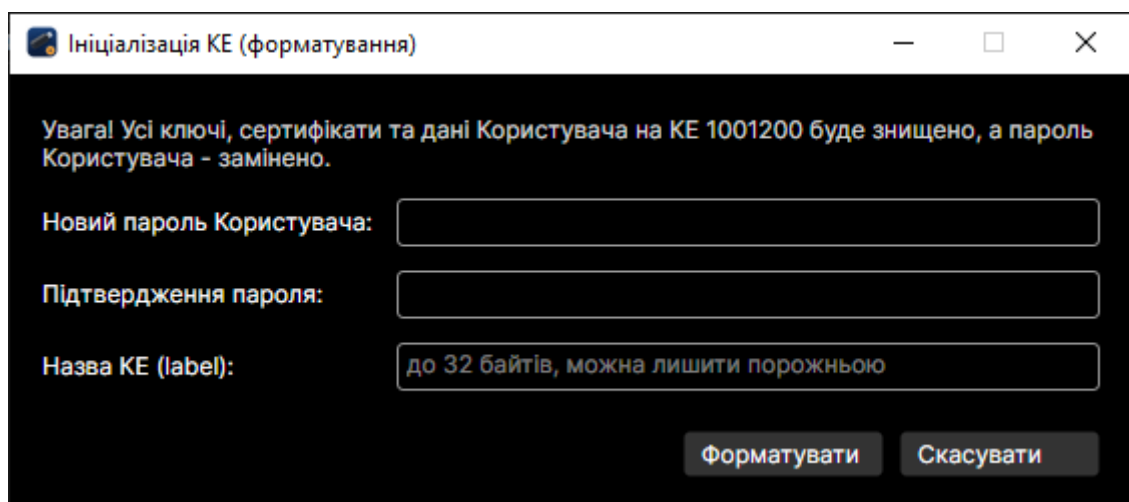


Рисунок 9 – Ініціалізація KE

Увага! Ініціалізація незворотно знищує всі ключі, сертифікати та дані Користувача на КЕ.

7.3 Параметри безпеки

Для зміни параметрів безпеки натисніть кнопку «Параметри безпеки». У діалоговому вікні (рис. 10) можна встановити:

- «Неправильних спроб входу до блокування Користувача» – кількість невдалих спроб автентифікації Користувача, після якої його обліковий запис блокується (від 1 до 100);
- «Властивості ключів лише для читання (заборонити зміну label та id)» – заборонити Користувачу змінювати назви та ідентифікатори ключів.

Для застосування змін натисніть клавішу Enter або кнопку «Встановити», для скасування – клавішу Esc або кнопку «Скасувати».

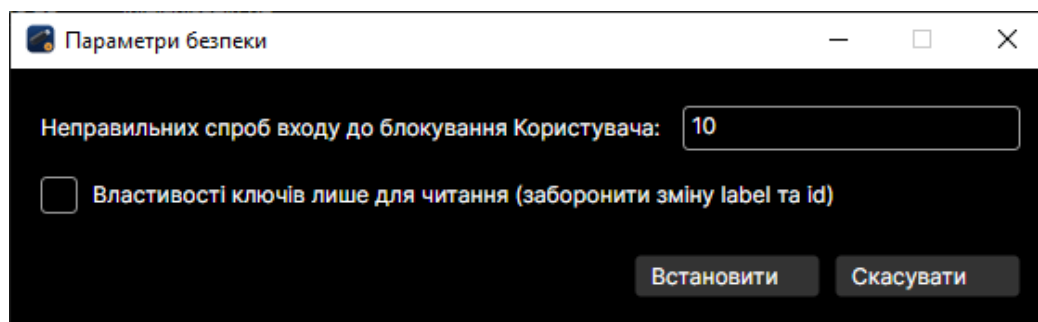


Рисунок 10 – Параметри безпеки

7.4 Розблокування

Для розблокування облікового запису Користувача натисніть кнопку «Розблокування». У діалоговому вікні (рис. 11) відображається поточний стан лічильника невдалих спроб входу Користувача. Для розблокування натисніть клавішу Enter або кнопку «Розблокувати», для скасування – клавішу Esc або кнопку «Скасувати». Розблокування скидає лічильник невдалих спроб, пароль Користувача при цьому не змінюється.

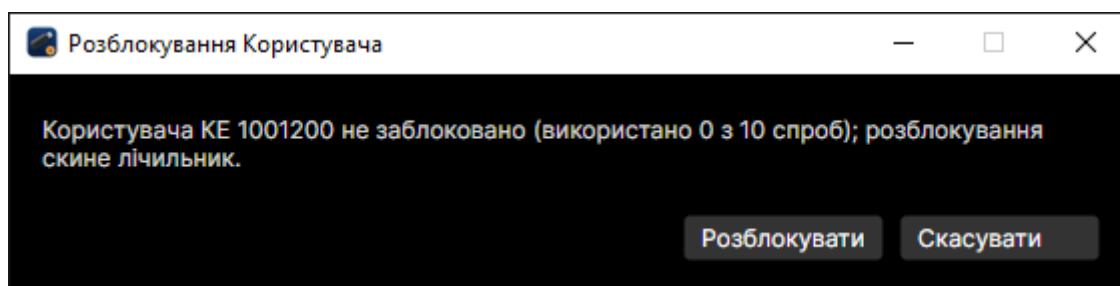


Рисунок 11 – Розблокування Користувача

7.5 Журнал подій

Журнал подій КЕ відображається в таблиці вікна Адміністратора безпеки (рис. 7). Колонки журналу:

- «N» – номер запису;
- «Дата і час» – час операції за годинником комп'ютера, з якого її виконано;
- «Операція» – назва операції;
- «Пар.» – параметр операції (шістнадцяткове значення);
- «Стор.» – номер сторінки пам'яті КЕ для операцій з ключами;
- «Ід. ключа» – перші байти ідентифікатора ключа.

Для відображення певної кількості останніх подій введіть число в поле «Останніх записів» і натисніть кнопку «Зчитати». Для відображення всіх подій натисніть кнопку «Весь журнал». Спроби входу журнал фіксує лише невдалі.

7.6 Вийти

Для завершення роботи в ролі Адміністратора безпеки та повернення до головного вікна натисніть кнопку «Вийти».

8. МОЖЛИВІ ПРОБЛЕМИ

Таблиця 4 – Можливі проблеми та способи їх усунення

Ситуація	Причина та дії
КЕ немає в переліку «Ключ електронний»	перевірте підключення КЕ та натисніть «Оновити перелік»; у Windows перевірте, що працює служба «Смарт-картка», у Linux – що встановлено й запущено pcsd і драйвер CCID (п. 3.2); у сеансі RDP див. п. 3.1
«Користувача заблоковано»	вичерпано кількість невдалих спроб входу; обліковий запис розблоковує Адміністратор безпеки (п. 7.4)
«Кнопку на токени не натиснуто протягом 30 секунд»	ключ потребує кнопки підтвердження; повторіть операцію та натисніть кнопку на КЕ, коли Утиліта про це попросить
Кнопка «Експорт» неактивна для ключа	ключ не має позначки «експортуємий» (е) і не може бути скопійований
Сертифікат не імпортується	на КЕ немає особистого ключа цього сертифіката або такий сертифікат там уже є (п. 6.3.2)
Не вдається змінити назву чи ідентифікатор ключа	мікропрограма КЕ старіша за 8.5 або Адміністратор безпеки заборонив зміну властивостей ключів (п. 7.3)
Неактивні алгоритм, параметр чи кнопка підтвердження у вікні генерації	модель або мікропрограма КЕ їх не підтримує (розділ 2)