ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
СПЕЦІНФОСИСТЕМИ

КЛЮЧ ЕЛЕКТРОННИЙ DIAMOND

УТИЛІТА НАЛАШТУВАННЯ ТА КЕРУВАННЯ

НАСТАНОВА КОРИСТУВАЧА

Версія 3.1

Харків – 2024

ЗМІСТ

1. ЗАГАЛЬНІ ВІДОМОСТІ

Утиліта налаштування та керування ключами електронними (КЕ) DIAMOND (далі – Утиліта) являє собою консольний програмний засіб призначений для:

- отримання детальної інформації про стан КЕ DIAMOND;
- зміни паролів Користувача та Адміністратора безпеки;
- розблокування заблокованого облікового запису Користувача;
- встановлення кількості невдалих спроб автентифікації Користувача до блокування його облікового запису;
- встановлення нового пароля Користувача (зі знищенням всіх даних Користувача);
- отримання переліку, створення (імпорту), зчитування (експорту) та знищення файлів з КЕ DIAMOND;
- перегляду журналу аудиту КЕ DIAMOND;
- створення та перевірки атестатів приватних ключів (підтвердження того, що приватний ключ згенеровано та зберігається засобом створення кваліфікованого підпису у відповідності до вимог нормативних документів щодо створення кваліфікованих підписів).

2. СИСТЕМНІ ВИМОГИ

Утиліта працює на наступних 64-х бітних операційних системах:

- Microsoft Windows 7 SP1 та новіше на платформі x86-64;
- macOS 12.0 та новіше на платформах x86-64 та arm64;
- Linux з встановленими пакетом libccid (Debian, Ubuntu та ін.) або pcsc-lite-ccid (Fedora, RedHat та ін.) версії 1.4.31 та новіше на платформах x86-64 та arm64.

3. ВСТАНОВЛЕННЯ ТА НАЛАШТУВАННЯ

Утиліта не потребує встановлення та налаштування.

Користувач, який запускає Утиліту повинен мати права доступу до USB пристроїв зчитування смарт-карток та до смарт-карток.

4. ОБЛІКОВІ ЗАПИСИ KE DIAMOND

В KE DIAMOND існують два облікових записи з відповідними функціональними можливостями: Користувач та Адміністратор безпеки.

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

Обліковий запис Користувача використовується для повсякденної роботи, а саме:

- генерації, використання та знищення приватних та таємних ключів криптографічних алгоритмів;
- створення атестатів приватних ключів;
- запису, зчитування та знищення приватних та публічних файлів, що містять довільні дані (сертифікати публічних ключів тощо);
- зміни власного паролю доступу.

Обліковий запис Адміністратора безпеки використовується для:

- встановлення кількості невдалих спроб автентифікації до блокування облікового запису користувача (в діапазоні від 1 до 100), після якої обліковий запис буде заблоковано;
- розблокування заблокованого облікового запису Користувача;
- встановлення нового пароля облікового запису Користувача зі знищенням всіх ключів та файлів користувача;
- зміни власного паролю доступу;
- перегляд журналу подій.

Заводські налаштування:

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

Увага! Заводські паролі облікових записів Адміністратора безпеки і Користувача мають бути змінені перед початком використання KE DIAMOND!

Увага! При втраті пароля Адміністратора безпеки використання KE DIAMOND буде обмежене, а при втраті паролів Адміністратора безпеки та Користувача використання KE DIAMOND за призначенням буде неможливе. Зберігайте пароль Адміністратора безпеки у спосіб, що забезпечує неможливість його втрати та компрометації!

5. РЕЖИМИ РОБОТИ

Утиліта працює в наступних режимах роботи, які впливають на доступність команд:

- КЕ DIAMOND не відкрито (режим Н);
- КЕ DIAMOND відкрито, авторизовану сесію не розпочато (режим НА);
- КЕ DIAMOND відкрито, сесія авторизованого Користувача (режим К);
- КЕ DIAMOND відкрито, сесія авторизованого Адміністратора безпеки (режим А).

В кожному режимі роботи запрошення до вводу команд відрізняються:

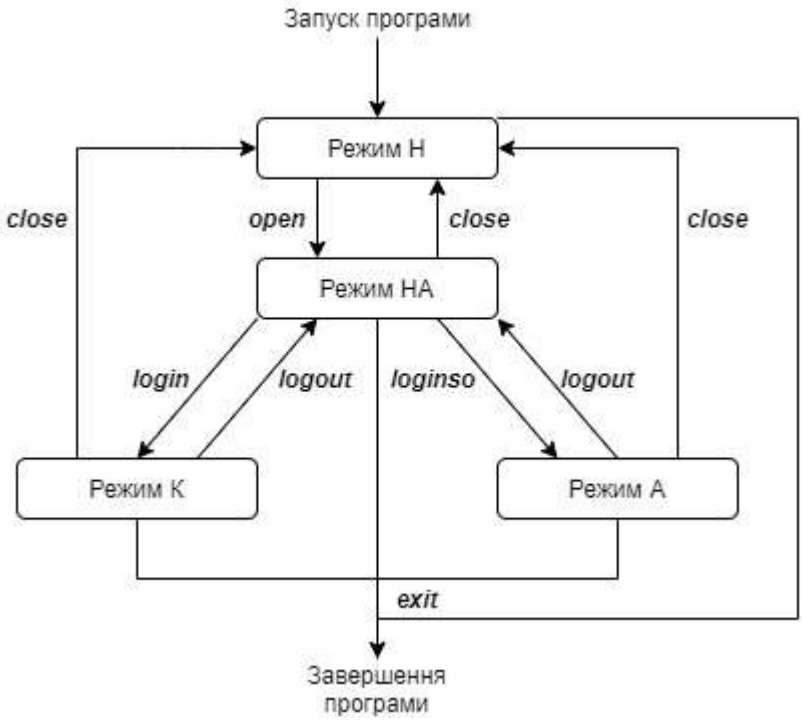
- режим Н: >
- режим НА: XXXXXXX[ ]>
- режим К: XXXXXXX[К]>
- режим Н: XXXXXXX[А]>

де XXXXXXX – серійний номер відкритого КЕ DIAMOND.

Перелік команд та їх доступність у кожному з режимів роботи наведені в таблиці 1. Діаграма роботи Утиліти та команди переключення станів зображені на малюнку 1.

Таблиця 1. Перелік команд та їх доступність команд в різних режимах роботи Утиліти

Команда	Режими роботи			
	Н	НА	К	А
?	+	+	+	+
help	+	+	+	+
list	+	+	+	+
exit	+	+	+	+
open	+			
login		+		
loginso		+		
logout			+	+
passwd			+	+
ls		+	+	+
rm			+	
import			+	
export		+	+	
readlog			+	+
format				+
unlock				+
attempts				+
pka			+	
vpka	+	+	+	+



Малюнок 1. Діаграма режимів роботи Утиліти

6. ПЕРЕЛІК КОМАНД

help або ***?***

Виводить перелік та короткий опис команд, доступних в поточному режимі роботи Утиліти.

Доступна у всіх режимах роботи.

exit

Завершає роботу Утиліти.
Доступна у всіх режимах роботи.

list

Виводить перелік підключених KE DIAMOND.
Доступна у всіх режимах роботи.

open

Відкриває KE DIAMOND та переводить Утиліту з режиму роботи H в режим HA. У разі, якщо підключено тільки один KE DIAMOND, він буде відкритий автоматично. Якщо підключено 2 та більше KE DIAMOND користувачу буде запропоновано обрати один з доступних шляхом введення його номеру у списку або серійного номеру.

Доступна у режимі роботи H.

info

Виводить інформацію про відкритий KE DIAMOND.
Доступна у всіх режимах роботи, крім H.

ls

Виводить перелік об’єктів (файлів та ключів) на відкритому KE DIAMOND та їх властивостей.

Доступна у всіх режимах роботи, крім H. У режимах HA та A виводить інформацію тільки про публічні об’єкти. У режимі K виводить інформацію про всі об’єкти (і публічні, і приватні).

Властивості об’єктів, що виводить програма: тип, атрибути, розмір або параметри, ідентифікатор ключа (обов’язково тільки для приватних ключів та сертифікатів публічних ключів) та додаток (не обов’язково), якого стосується цей об’єкт. В KE DIAMOND існують наступні типи об’єктів:

«ключ» - приватний або таємний ключ;
«пуб.к» - публічний ключ;
«серт» - сертифікат публічного ключа;
«дані» - файл з довільними даними.

Об’єкти типу «ключ» можуть бути тільки приватними, інші типи об’єктів можуть бути як приватними, так і публічними. Приватні об’єкти в полі атрибут мають позначку *.

Можливі атрибути об’єктів типу «ключ»:

e – можливий експорт з KE DIAMOND;

d – може використовуватись в протоколі узгодження ключів (для алгоритмів на еліптичних кривих);

b – для запуска процесу формування електронних підписів потрібне підтвердження присутності користувача шляхом натискання ємнісної кнопки (обробляється тільки моделями KE DIAMOND 3000 та 4000);

s – при формування кожного електронного підпису потрібне підтвердження присутності користувача шляхом натискання ємнісної кнопки (обробляється тільки моделями KE DIAMOND 3000 та 4000).

Параметри об’єктів типу «ключ»: для приватних ключів алгоритмів на еліптичних кривих – алгоритм та назва еліптичної кривої, для приватних ключів RSA – алгоритм та довжина параметра n в бітах, для таємних ключів блочних симетричних шифрів – алгоритм та довжина ключа в бітах.

Для всіх інших об’єктів, крім типу «ключ» виводиться: назва, тип, розмір у байтах, атрибут приватний/публічний, ідентифікатор публічного ключа та додаток (не обов’язково) яких стосується цей об’єкт.

login

Розпочинає сесію Користувача та переводить Утиліту з режиму роботи НА в режим К. Після вводу команди користувачу буде запропоновано ввести пароль облікового запису Користувача відкритого KE DIAMOND. Під час вводу пароль відображається символами *.

Доступна тільки в режимі НА.

loginso

Розпочинає сесію Адміністратора безпеки та переводить Утиліту з режиму роботи НА в режим А.

Після вводу команди користувачу буде запропоновано ввести пароль облікового запису Адміністратора безпеки відкритого KE DIAMOND. Під час вводу пароль відображається символами *.

Доступна тільки в режимі НА.

logout

Завершує сесію Користувача або Адміністратора безпеки та переводить Утиліту в режим роботи НА.

Доступна тільки в режимах К та А.

close

Закриває відкритий KE DIAMOND та переводить Утиліту в режим роботи Н.

Доступна у всіх режимах роботи, крім Н.

rm

Знищує (видаляє) об’єкт (ключ або файл) з пам’яті KE DIAMOND.

Після вводу команди буде виведено перелік об’єктів на KE DIAMOND і користувачу буде запропоновано ввести номер об’єкту для знищення.

Доступна в режимі роботи К.

import

Створює об’єкт в пам’яті KE DIAMOND шляхом копіювання з файлу на ПЕОМ.

Після вводу команди користувачу буде запропоновано ввести ім’я файлу для імпорту. У разі, якщо файл знаходиться не в поточному каталозі, ім’я файлу необхідно вказати з повним або відносним шляхом.

Утиліта може створити об’єкт типу «дані» або сертифікат («серт»). Тип об’єкту визначається автоматично за вмістом файлу на ПЕОМ. При створенні об’єкту типу «дані» користувачу буде запропоновано ввести ім’я об’єкту, додаток, якого стосується об’єкт (не

обов'язково), та визначити атрибут доступу до об'єкту: публічний чи приватний. При створенні об'єкту типу сертифікат («серт») користувачу буде запропоновано тільки визначити атрибут доступу до об'єкту: публічний чи приватний, інші атрибути будуть заповнені автоматично. Для сертифікатів рекомендується встановлювати атрибут доступу «публічний».

Доступна в режимі роботи К.

export

Зчитує об'єкт з пам'яті КЕ DIAMOND та зберегти його у файл на ПЕОМ. Для об'єктів типу «ключ» з можливістю експорту зберігання виконується на інший або той самий КЕ DIAMOND.

Після вводу команди буде виведено перелік об'єктів на КЕ DIAMOND і користувачу буде запропоновано ввести номер об'єкту для експорту.

Якщо здійснюється експорт інших ніж «ключ» типів об'єктів, користувачу буде запропоновано ввести ім'я файлу для збереження. Якщо файл необхідно зберегти не в поточному каталозі, необхідно вказати ім'я файлу з повним або відносним шляхом. По замовчанню (у разі натискання Enter без вводу імені файлу), буде збережено файл у поточному каталозі з іменем, що збігається з номером об'єкту у виведеному переліку.

Якщо експорт виконується експорт об'єкту типу «ключ», програма виведе список підключених КЕ DIAMOND та користувачу буде запропоновано вибрати КЕ DIAMOND, на який буде скопійовано ключ. При виконанні операції користувач має вказати нове ім'я та нові атрибути ключа. Допустимо вибирати той самий КЕ DIAMOND, з якого експортується ключ, при цьому необхідно вказати нове ім'я об'єкту, що відрізняється від старого. Обидва КЕ DIAMOND (з якого та на який копіюються ключ) мають бути підключені до ЕОМ одночасно до завершення виконання команди.

Доступна в режимі роботи К.

passwd

Встановити новий пароль облікового запису КЕ DAIMOND (Користувача в режимі роботи К або Адміністратора безпеки в режимі роботи А). В процесі виконання користувачу буде запропоновано ввести новий пароль та його підтвердження. Під час вводу пароль та підтвердження відображаються символами *.

Доступна в режимах роботи К та А.

readlog

Вивести журнал подій. Оскільки КЕ DIAMOND не має вбудованого годинника, час подій в журналі встановлюється відповідно до системного часу на ПЕОМ, до якої під'єднано КЕ DIAMOND. В журналі зберігається інформація про наступні події:

- невдалі спроби автентифікації Користувача (LOGIN);
- невдалі спроби автентифікації Адміністратора безпеки (LOGIN S);
- генерація об'єктів типу «ключ» (GEN KEY);
- імпорт об'єктів типу «ключ» (IMP KEY);
- експорт об'єктів типу «ключ» (EXP KEY);
- знищення об'єктів типу «ключ» (DEL KEY);
- встановлення кількості невдалих спроб автентифікації до блокування облікового запису Користувача (SET SP);
- зміна пароля облікового запису (PASSWD). Тип облікового запису зберігається в параметрі 1 – Користувач, 2 – Адміністратор безпеки;
- копіювання ключа (CP KEY);
- розблокування облікового запису користувача (UNLOCK);

- ініціювання облікового запису Користувача зі знищенням всіх даних Користувача (INIT CO);
- ініціалізація облікового запису Адміністратора безпеки (виконується виробником одноразово) (INIT SO).

Доступна в режимах роботи К та А.

format

Ініціює обліковий запис Користувача та знищує всі дані Користувача в пам'яті КЕ DIAMOND. В процесі виконання користувачу буде запропоновано ввести новий пароль та його підтвердження. Під час вводу пароль та підтвердження відображаються символами *. Операцію рекомендується виконувати у разі передачі КЕ DIAMOND іншому користувачу та у разі, якщо користувач не може згадати пароль доступу до облікового запису Користувача.

Доступна в режимі роботи А.

unlock

Розблоковує обліковий запис Користувача.

Доступна в режимі роботи А.

attempts

Встановлює кількість невдалих спроб автентифікації Користувача до блокування його облікового запису. Після вводу команди користувачу буде запропоновано ввести нове значення цього параметру. Може бути встановлено в діапазоні від 1 до 100.

Доступна в режимі роботи А.

pka

Створення атестата приватного ключа.

Після успішного виконання атестат буде виведено на екран у шістнадцятковому вигляді та користувачу буде запропоновано зберегти його у файл. Якщо користувач вибере так (yes), потрібно буде ввести ім'я файлу для збереження атестата. У разі, якщо файл потрібно зберегти не в поточному каталозі, ім'я файлу необхідно вказати з повним або відносним шляхом.

Атестат приватного ключа дозволяє стороннім особам (зазвичай центрам сертифікації ключів) впевнитись, що відповідний приватний ключ був згенерований без можливості екстракції засобом створення кваліфікованих підписів без фізичного доступу до такого засобу. Атестат може бути сформований тільки для приватних ключів алгоритмів ДСТУ-4145, ECDSA, RSA, які були згенеровані КЕ DIAMOND і не мають можливості експорту (екстракції).

Доступна в режимі роботи К.

vpka

Перевіряє атестат приватного ключа.

Після запуску команди користувачу буде запропоновано ввести ім'я файлу на ПЕОМ з атестатом, або сам атестат, заданий у шістнадцятковому вигляді. У разі успішної перевірки виводить ідентифікатор публічного ключа, тип та серійний номер засобу створення кваліфікованих підписів, у якому було згенеровано та зберігається відповідний приватний ключ.

Доступна у всіх режимах роботи.

7. ПОРЯДОК ТА ПРИКЛАДИ ВИКОНАННЯ ОПЕРАЦІЙ

Підключіть КЕ DIAMOND, з яким плануєте виконувати операції, до USB порту ПЕОМ та запустіть Утиліту. Робота з Утилітою відбувається в командно-діалоговому режимі шляхом вводу команд та відповідей на запитання програми і натискання кнопки Enter після вводу команди або відповіді. Для команд підтримується автодоповнення по натисканню кнопки Tab.

Зміна паролю облікового запису Користувача

1. Відкрийте ключ – команда ***open***
2. Розпочніть сесію Користувача – команда ***login***
3. Виконайте зміну паролю – команда ***passwd***
4. Завершіть роботу з програмою – команда ***exit***

Зміна паролю облікового запису Адміністратора безпеки

1. Відкрийте ключ – команда ***open***
2. Розпочніть сесію Адміністратора безпеки – команда ***loginso***
3. Виконайте зміну паролю – команда ***passwd***
4. Завершіть роботу з програмою – команда ***exit***

Ініціалізація облікового запису Користувача

1. Відкрийте ключ – команда ***open***
2. Розпочніть сесію Адміністратора безпеки – команда ***loginso***
3. Виконайте ініціалізацію облікового запису Користувача – команда ***format***
4. Завершіть роботу з програмою – команда ***exit***

Розблокування облікового запису Користувача

1. Відкрийте ключ – команда ***open***
2. Розпочніть сесію Адміністратора безпеки – команда ***loginso***
3. Виконайте розблокування облікового запису Користувача – команда ***unlock***
4. Завершіть роботу з програмою – команда ***exit***

Формування атестата приватного ключа

1. Відкрийте ключ – команда ***open***
2. Розпочніть сесію Користувача – команда ***login***
3. Виконайте формування атестата – команда ***pka***
4. Завершіть роботу з програмою – команда ***exit***

Перевірка атестата приватного ключа

1. Виконайте перевірку атестата – команда ***vpka***
2. Завершіть роботу з програмою – команда ***exit***