ПФ «Енігма-Софт»

61072, Україна, м. Харків, вул. 23 Серпня 38, к. 23.
http://enigmasoft.com.ua, office@enigmasoft.com.ua
+380-577-177-977, +380-577- 590-723,+380-577-590-724
+380-50-30-15-155, +380-97-96-14-231, +380-93-30-15-155

Комплекс «Стиль» - Клієнт-Банк

Захищені носії ключів

Інструкція з експлуатації

Харків

Зміст

1. Введення

Даний документ призначений для користувачів **«Стиль» - Клієнт-Банк** з системою захисту х.509 **ІІТ**.

Документ покликаний допомогти користувачам у виборі оптимального носія ключів.

Опис відповідає версії **«Стиль» - Клієнт-Банк** версії 4.47.012 або вище, що працює під управлінням ОС Windows XP sp3 або вище.

1.1. Особливості роботи під Windows XP

Робота з Windows XP ведеться аналогічно роботі на Windows 7, 8,10.

Примітка: при виникненні проблем з роботою носіїв електронних ключів, необхідно переконається, що в системі присутній драйвер **«Пристрій читання смарт-карт» (Usbccid.sys)**. В разі його відсутності, необхідно встановити компонент, за допомогою сервера оновлень Microsoft (windowsupdate.microsoft.com).

Робота на Windows XP під віртуальною машиною (Vmware)

Підтверджена робота всіх ключів, окрім Aladdin Jacarta (можуть виникнути проблеми при інсталяції супутніх бібліотек і утиліт).

2. Захищені носії ключів

2.1. Робота з електронним ключем «Автор»

Зовнішній вигляд ключа представлений на Зобр.1

Зображення 1.Ключ Avtor secure token 337.

Попереднє налаштування

ОС при підключенні пристрою в USB-порт визначає пристрій і встановлює необхідні драйвери автоматично.

PIN-код пристрою

Для будь-яких операцій з пристроєм, необхідно знати його PIN-код.

Передвстановлений: *«12345678».*

У системі **«Стиль» - Клієнт-Банк** пароль доступу до особистого ключа посадової особи і PIN-код збігаються.

При генерації ключа на пристрій обов'язково вводиться пароль ключа, рівний значенню PIN-кода пристрою.

Наступним кроком пароль ключа і PIN-код пристрою змінюються, функцією зміни пароля в системі захисту комплексу **«Стиль» - Клієнт-Банк**.

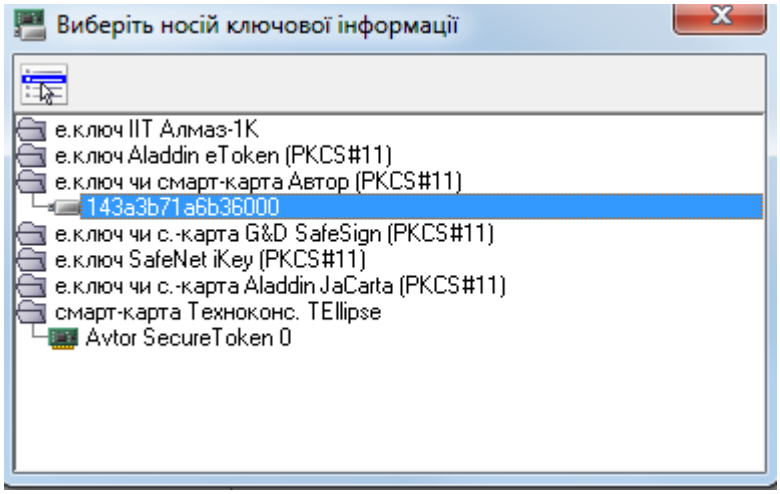
В разі втрати PIN-кода пристрою, початкові налаштування пристрою відновлюються за допомогою спеціальних утиліт, що надаються виробником за запитом.

Робота з пристроєм

Для вказівки пристрою в комплексі «Стиль» - Клієнт банк необхідно:

- Підключити пристрій до USB-порту;
- Вибрати типа носія - **«smart-карта»**;
- Вибрати в списку пристрій, що відображується як**«е.ключ чи смарт-карта Автор (PKCS#11) - «Код носія»»** (Див. Зобр.2)

Увага! Робота з пристроєм, що відображується як **«smart карта Техноконс. TEllipse - Avtor secure token 0»** заборонена.



Зображення 2.Вибір носія ключової інформації.

Функції управління ключами

ДДоступні наступні функції управління ключем на пристрої:

- Перегляд контексту ключа;
- Зміна пароля ключа;
- Видалення ключа з носія;

Заборонені наступні функції управління ключем на пристрої:

- Резервне копіювання ключа з носія;
- Резервне копіювання ключа на носій;

2.2. Робота з електронним ключем «Алмаз 1К»

Зовнішній вигляд ключа представлений на Зобр.3

Зображення 3. Електронний ключ «Алмаз -1К».

Попереднє налаштування

ОС при підключенні пристрою в USB-порт визначає пристрій і встановлює необхідні драйвери автоматично.

PIN-код пристрою

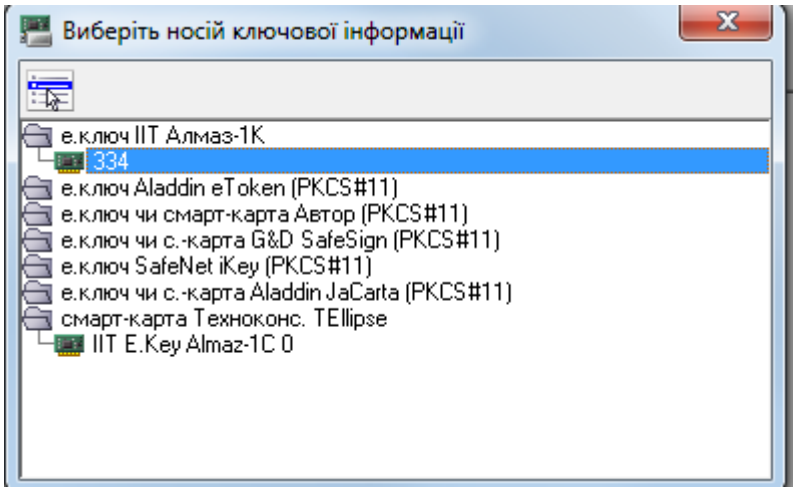
Для роботи з фінансовими документами необхідно знати PIN-код пристрою.
У системі **«Стиль» - Клієнт-банк** пароль доступу до особистого ключа посадової особи і PIN-код збігаються.
Передвстановлений PIN-код пристрою відсутній. Пароль ключа, введений при генерації, встановлюється PIN-кодом пристрою і надалі робота ведеться з ним.
При генерації нового ключа з новим паролем, старий ключ і пароль видаляються.

Робота з пристроєм

Для вказівки пристрою в комплексі **«Стиль» - Кклієнт-Банк** необхідно:

- Підключити пристрій до USB-порту;
- Вибрати типа носія - **«smart-карта»**;
- Вибрати в списку пристрій що відображується як «**е.ключ ІІТ Алмаз – 1К - «Код носія»**» (Див. Зобр.4)

Увага! Робота з пристроєм, що відображується як **«smart карта Техноконс. TEllipse - «ІІТ E.Key Almaz-1C 0»»** заборонена.



Зображення 4.Вибір носія ключової інформації.

Функції управління ключами

Доступні наступні функції управління ключем на пристрої:

- Перегляд контексту ключа;
- Зміна пароля ключа;
- Видалення ключа з носія;

Заборонені наступні функції управління ключем на пристрої:

- Резервне копіювання ключа з носія;
- Резервне копіювання ключа на носій;

2.3. Робота з електронним ключем «Кристал-1»

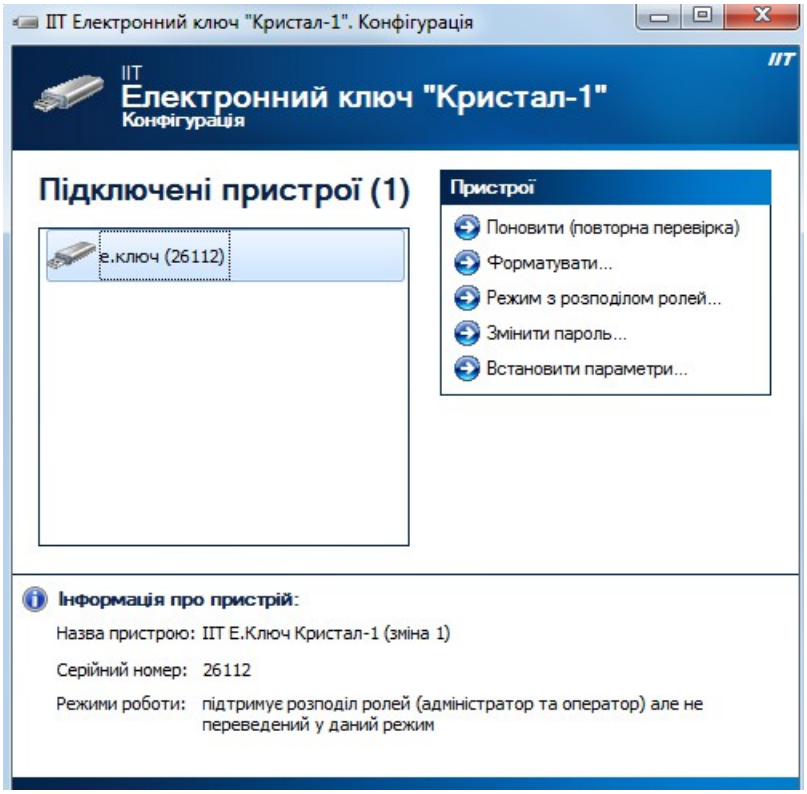
Зовнішній вигляд ключа представлений на Зобр.5

Зображення 5.Електронний ключ Кристал-1.

Попереднє налаштування

Перед початком використання пристрою, на ПК клієнта необхідно:

- Встановити призначене для користувача ПЗ пристрою «ІІТ Е.ключ Крістал-1», доступне за наступною адресою: (http://iit.com.ua/download/productfiles/EKeyCrystal1Install.exe);
- Підключити пристрій до USB-порту;
- Виконати ініціалізацію (форматування) пристрою і встановити PIN-код пристрою з допомогою, встановленого ПЗ (Див. Зобр. 6);



Зображення 6. Программа «ІІТ е.ключ Кристал-1».

PIN-код пристрою

Для будь-яких операцій з пристроєм, необхідно знати його PIN-код.

Початковий PIN-код пристрою задається при ініціалізації пристрою.

В системі **«Стиль» - Клієнт-Банк** пароль доступу до особистого ключа посадової особи і PIN-код збігаються.

При генерації ключа на пристрій обов'язково вводиться пароль ключа, рівний значенню PIN-кода пристрою.

Наступним кроком пароль ключа і PIN-код пристрої змінюються, функцією зміни пароля в системі захисту комплексу **«Стиль» - Клієнт-Банк**.

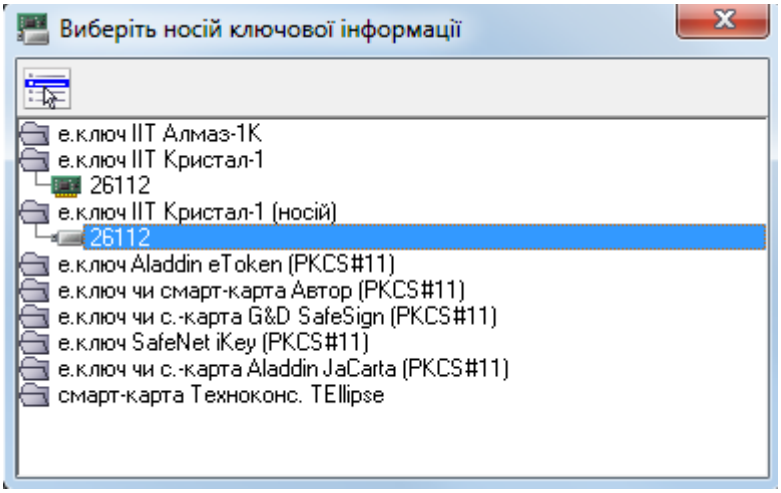
В разі втрати PIN-кода пристрою, виконати ініціалізацію і встановити PIN-код пристрою з допомогою, встановленого ПЗ (Див. Зобр. 6).

Робота з пристроєм

Для вказівки пристрою в комплексі **«Стиль» - Клієнт-Банк** необхідно:

- Підключити пристрій доUSB-порту;
- Вибрати типа носія - **«smart-карта»**;
- Вибрати в списку пристрій, що відображується як « **е.ключ Кристал - 1 - «Код носія»»** (Див. Зобр.7) або « **е.ключ Кристал - 1 (носій) - «Код носія»»**;

Увага! Обидва елементи списку адресують один і той же пристрій і операції з будь-яким з елементів тотожні.



Зображення 7.Вибір носія ключової інформації.

Функції управління ключами

Доступні наступні функції управління ключем на пристрої:

- Перегляд контексту ключа;
- Зміна пароля ключа;
- Видалення ключа з носія;

Заборонені наступні функції управління ключем на пристрої:

- Резервне копіювання ключа з носія;
- Резервне копіювання ключа на носій;

2.4. Робота з електронним ключем «SafeNet 5100»

Зовнішній вигляд ключа представлений на Зобр.8

Зображення 8. Електронний ключ «SafeNet 5100».

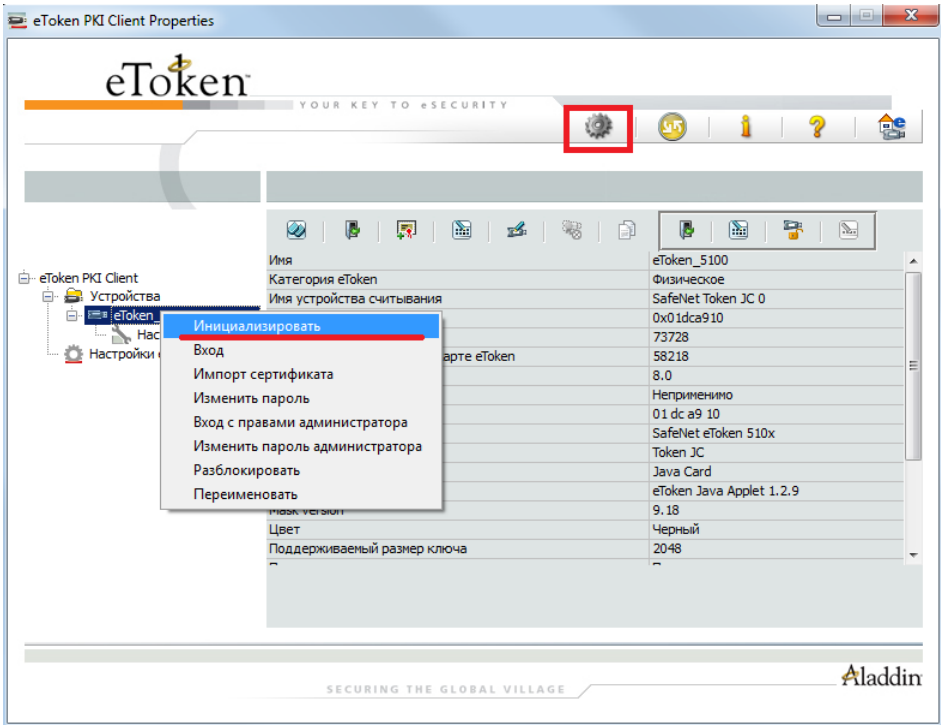
Попереднє налаштування

УПристрій поставляється з платним ПЗ (Security authentication Client) від виробника з ліцензією, що оновлюється щорічно. Ліцензії від виробника на дане ПЗ за час тестування

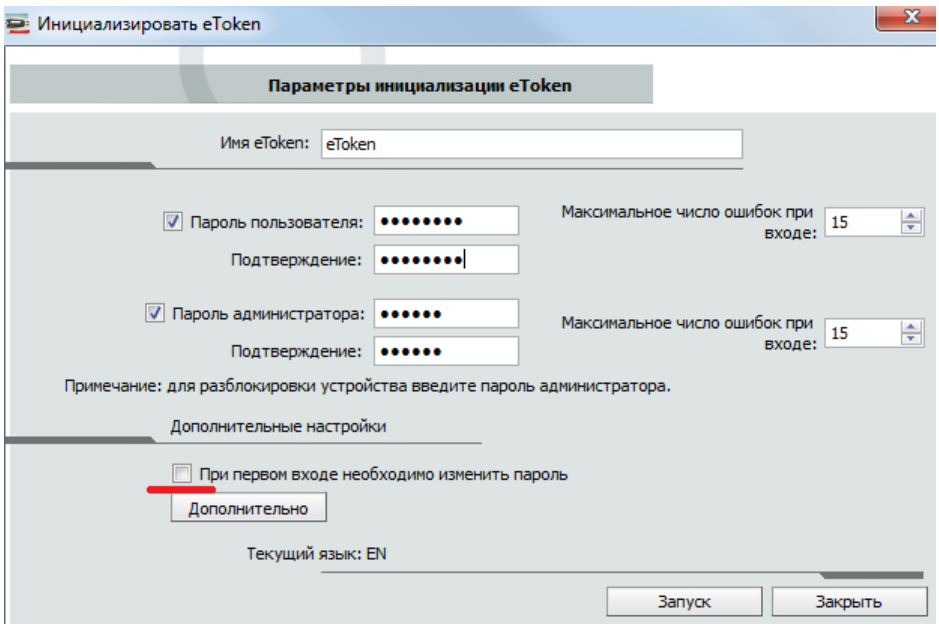
пристрою ми так і не отримали, не дивлячись на своєчасну оплату.

- Встановлено альтернативне, безкоштовне ПЗ **«eToken PKI client 5.1», надане постачальником електронних ключів;**
- Виконати ініціалізацію (форматування) пристрою з допомогою встановленого ПЗ (Див. Рис 9,10);
- Встановити PIN-коди адміністратора і користувача, без налаштування зміни пароля при першому запуску і натиснути «Запуск»;

Детальна документація надається продавцем і виробником пристрою.



Зображення 9. Ініціалізація «SafeNet 5100» з допомогою «eToken PKI client 5.1».



Зображення 10.Вибір параметрів ініціалізації «SafeNet 5100» з допомогою «eToken PKI client 5.1».

PIN-код пристрою

Для будь-яких операцій з пристроєм, необхідно знати його PIN-код.

PIN-код користувача і адміністратора задаються при ініціалізації пристрою. (Зобр.9,10)

В системі **«Стиль» - Клієнт-Банк** пароль доступу до особистого ключа посадової особи і PIN-код користувача збігаються.

В разі втрати PIN-кода користувача, доступ до ключа посадової особи буде загублений.

Після 15 невірних спроб введення пароля (параметр, що набудовується при ініціалізації) доступ до ключа посадової особи по PIN-коду користувача буде заблокований.

Щоб продовжити роботу з пристроєм, необхідно його повторно ініціалізувати.

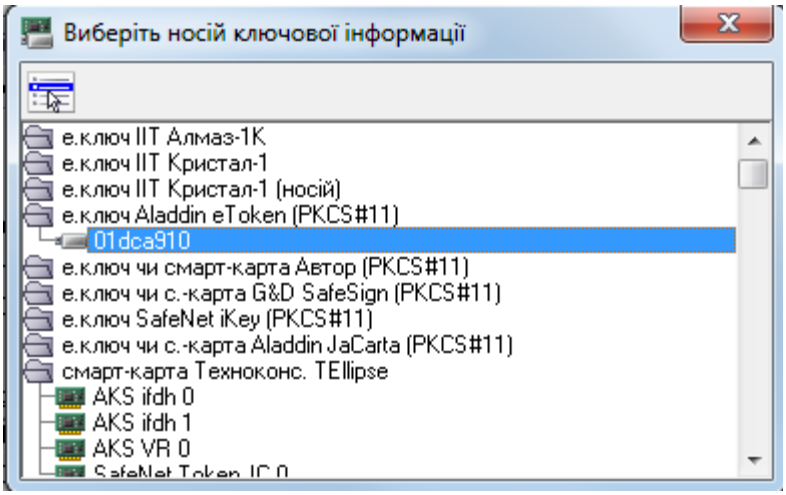
При втраті обох PIN-кодів, пристрій необхідно повторно ініціалізувати, при цьому всі дані на пристрої будуть загублені.

Робота з пристроєм

Для вказівки пристрою в комплексі «Стиль» - Клієнт Банк необхідно:

- Підключити пристрій до USB-порту;
- Вибрати тип носія - **«smart-карта»**;
- Вибрати в списку пристрій, що відображується як « **е.ключ Aladdin eToken (PKCS#11) - «Код носія»»** (Див. Зобр.11)

Увага! Робота зі всіма пристроями окрім « **е.ключ Aladdin eToken (PKCS#11) - «Код носія»»** заборонена.



Зображення 11.Вибір носія ключової інформації.

Функції управління ключами

Доступні наступні функції управління ключем на пристрої:

- Перегляд контексту ключа;
- Зміна пароля ключа (За умовчанням лише «сильний» буквено-цифровий пароль в різних регістрах. Вимоги до стійкості ключа, можуть бути налаштовані в утиліті конфігурації пристрою («eToken PKI client 5.1»). В разі неспівпадання нового пароля, зконфігурованим критеріям, виникає помилка-17 (0x0011));
- Видалення ключа з носія;

Заборонені наступні функції управління ключем на пристрої:

- Резервне копіювання ключа з носія;
- Резервне копіювання ключа на носій;

2.5. Робота з електронним ключем «JaCarta»

Зовнішній вигляд ключа представлений на Зобр.12

Зображення 12. Електронний ключ «Aladdin JaCarta».

Попереднє налаштування

Перед початком використання пристрою, на ПК клієнта необхідно:

- Встановити призначене для користувача ПЗ пристрою «Jacarta DSTU», надається виробником;
- Підключити пристрій до USB-порту;
- Виконати ініціалізацію (форматування) пристрою з допомогою встановленого ПЗ (Див. Рис 13);
- Встановити PIN-код адміністратора на 3-ій вкладці «Ініціалізація» (передвстановлений код «1234567890»);
- Ініціалізувати PIN-код користувача, не менше 6 символів (вкладка 2, операції з «ПІН-кодом»);

Детальна документація надається продавцем і виробником пристрою.

Зображення 13.Ініціалізація PIN-кода адміністратора і користувача.

PIN-код пристрою

Для будь-яких операцій з пристроєм в комплексі «Стиль» - Клієнт-банк, необхідно знати його PIN-код користувача.

PIN-код користувача і адміністратора задаються при ініціалізації пристрою. (Зобр.13)

У системі **«Стиль» - Клієнт-Банк** пароль доступу до особистого ключа посадової особи і PIN-код користувача збігаються.

При втраті PIN-кода користувача, доступ до ключа посадової особи буде загублений. Для подальшої роботи з пристроєм, необхідно буде знову провести ініціалізацію пристрою.

Після 10 невірних спроб введення пароля користувача, пристрій блокується. Для роботи із старим PIN-кодом, необхідно розблоковувати пристрій за допомогою пароля адміністратора.

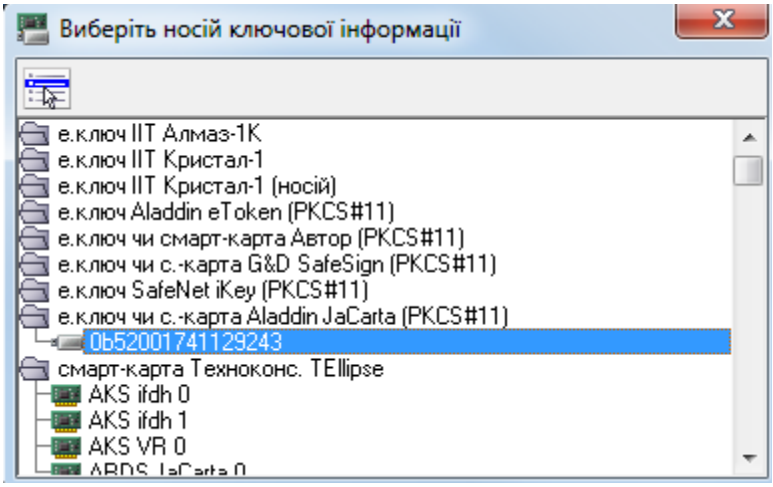
Після 10 невірних спроб введення пароля адміністратора, пристрій, і всі операції, з правами адміністратора блокуються і не можуть бути відновлені.

Робота з пристроєм

Для вказівки пристрою в комплексі **«Стиль» - Клієнт-Банк** необхідно:

- Підключити пристрій до USB-порту;
- Вибрати типа носія **- «smart-карта»**;
- Вибрати в списку пристрій, що відображується як « **е.ключ чи с.-карта Aladdin JaCarta (PKCS#11) - «Код носія»»** (Див. Зобр.14) ;

Увага! Робота зі всіма пристроями, окрім « **е.ключ чи с.-карта Aladdin JaCarta (PKCS#11)- - «Код носителя»»** заборонена.



Зображення 14.Вибір носія ключової інформації.

Функції управління ключами

Доступні наступні функції управління ключем на пристрої:

- Перегляд контексту ключа;
- Зміна пароля ключа;
- Видалення ключа з носія;

Заборонені наступні функції управління ключем на пристрої:

- Резервне копіювання ключа з носія;
- Резервне копіювання ключа на носій;

Фахівці ПФ «Енігма-Софт» бажають Вам
ПРИЄМНОЇ РОБОТИ