

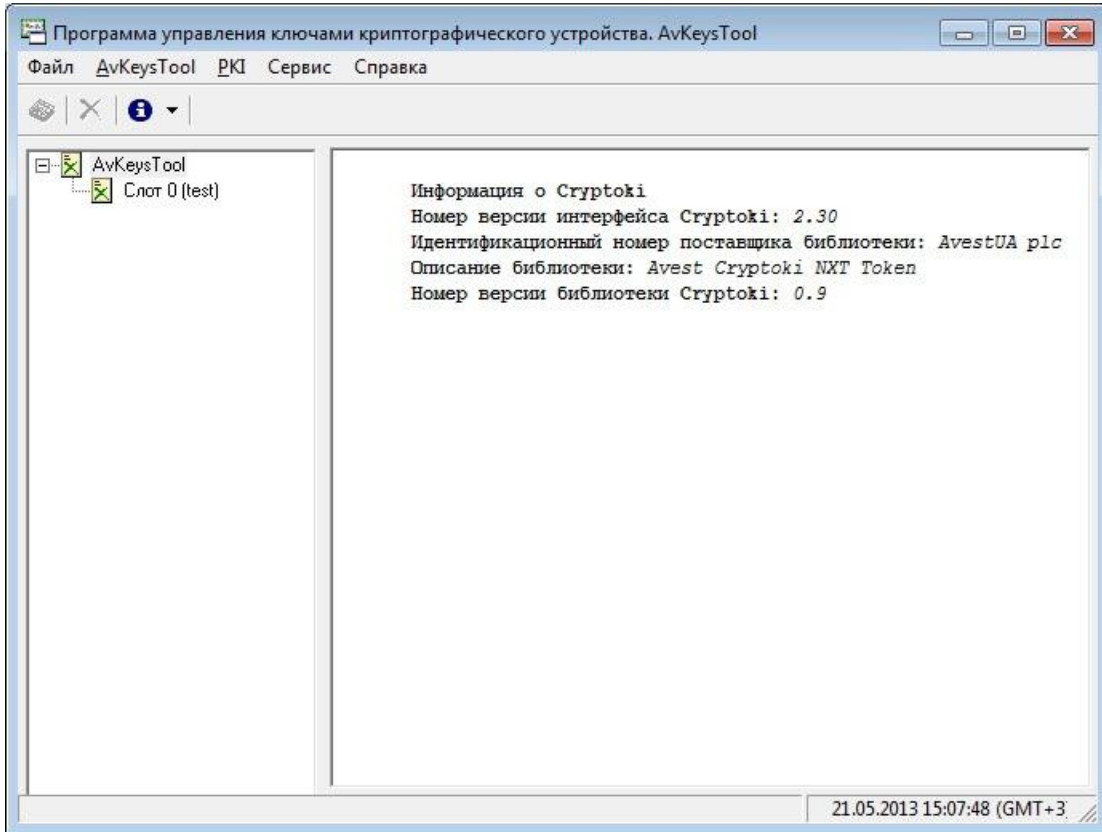
Робота з AvKeysTool

Для запуску програми AvKeysTool необхідно виконати наступні дії:

Вибрати в меню «Пуск» ОС Windows пункти «Програми» - «AvestKey Tools» - AvKeysTool», або двічі клацнути на іконці програми, розташованій на робочому столі;

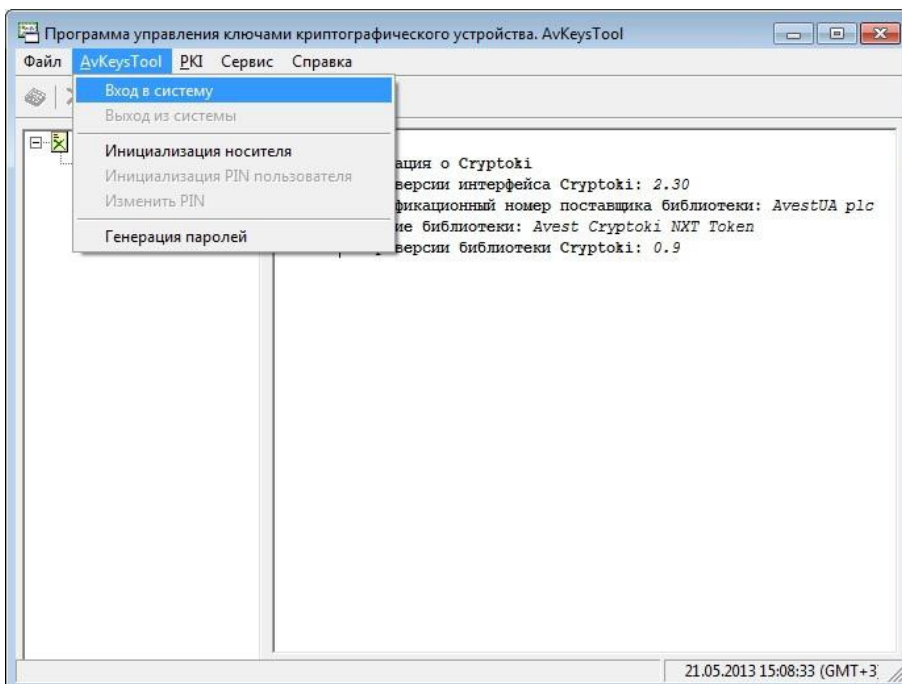


Програма підключиться до пристрою AvestKey і відобразить на екрані головне вікно програми (див. Малюнок 1).

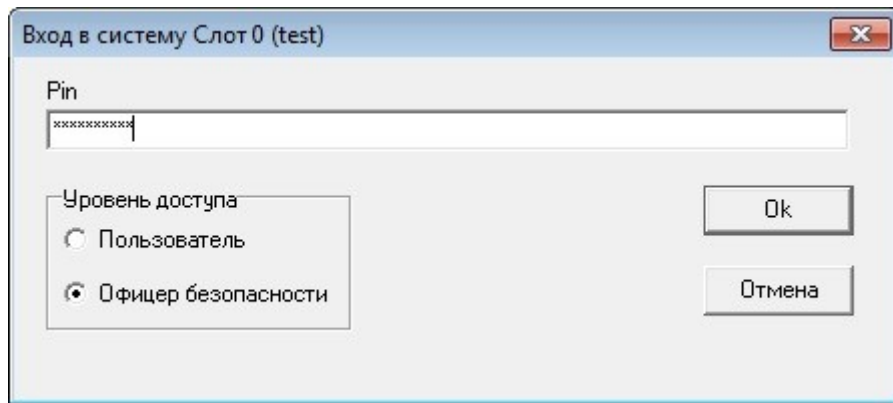


Малюнок 1. Головне вікно AvKeysTool

Вхід в AvKeysTool можливий у двох режимах: Офіцера безпеки та Користувача (див. Малюнок 2, Малюнок 3).

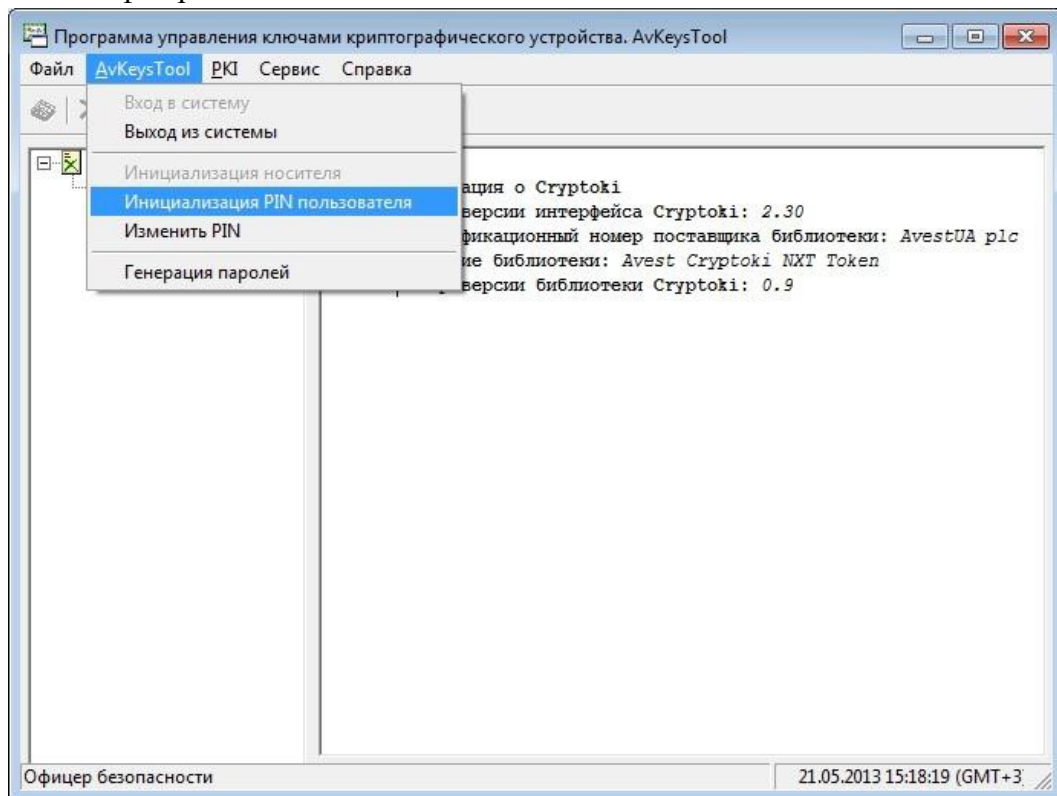


Малюнок 2. Вхід в систему



Малюнок 3. Вхід в систему Офіцера безпеки

Використовуваний проініціалізований носій вже містить слот test і дві облікові записи: Офіцера безпеки з паролем 1234567890 та Користувача з паролем 12345678. Режим Офіцера безпеки дозволяє знову переініціалізувати Користувача і задати йому PIN-код або змінити поточний PIN-код Офіцера безпеки.

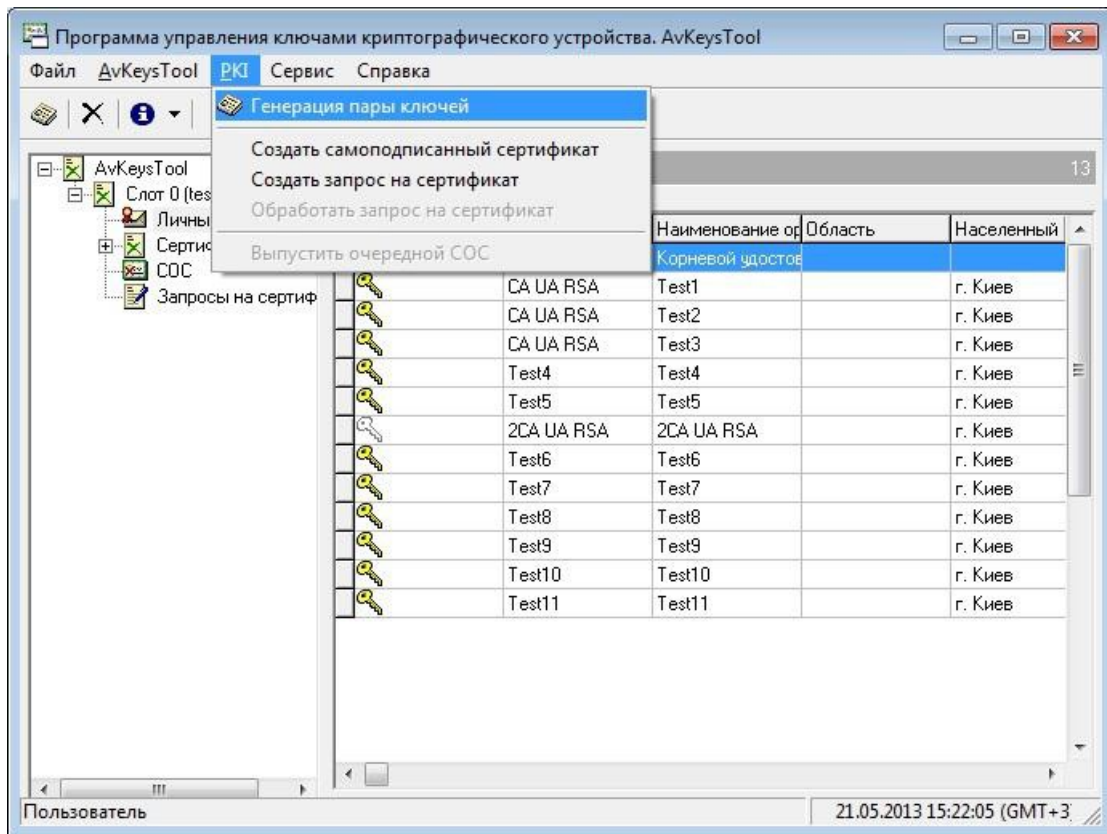


Малюнок 4. Ініціалізація PIN Користувача

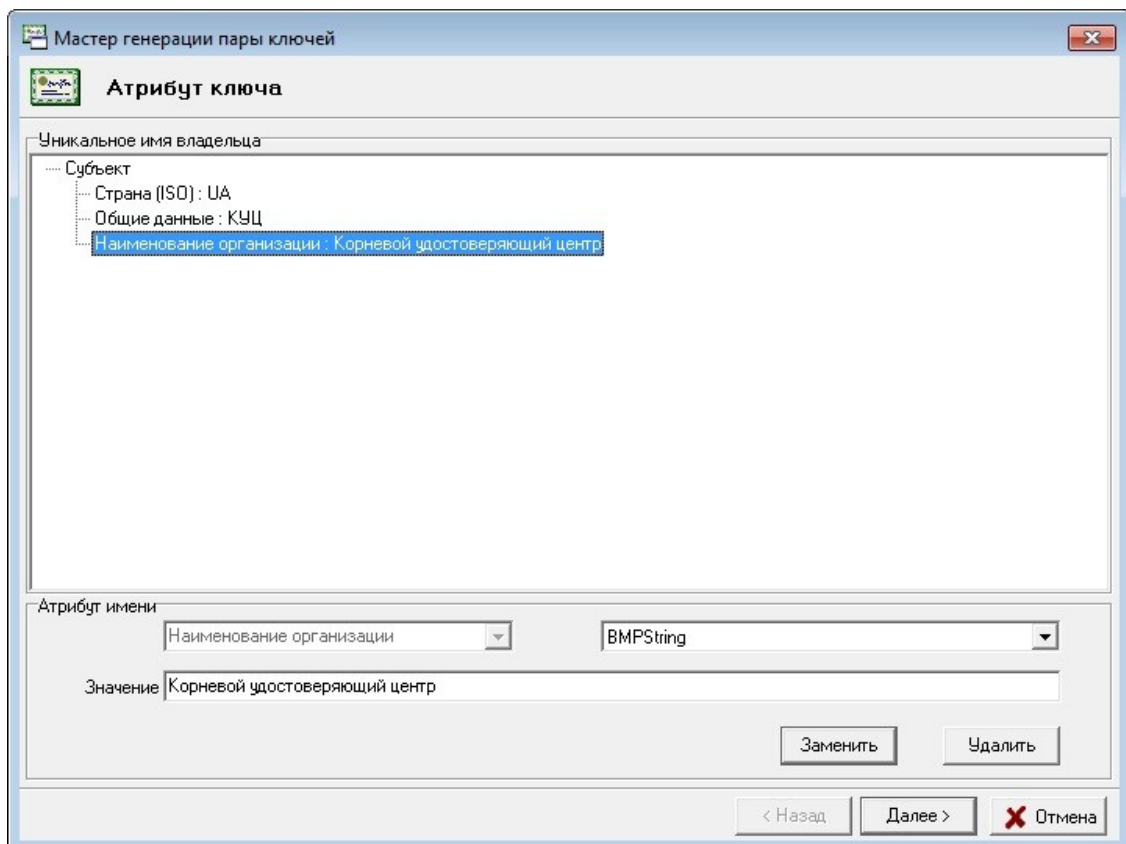
Робота з PKI-компонентами AvKeysTool

Основна робота з PKI-компонентами AvKeysTool відбувається в режимі Користувача. Для цього потрібно спочатку здійснити вихід із системи Офіцера безпеки: меню «AvKeysTool - Вихід із системи» і увійти використовуючи режим Користувача.

У режимі користувача нам стає доступне меню «PKI - Генерація ключів» і ми можемо створити Корневий самопідписаний сертифікат.



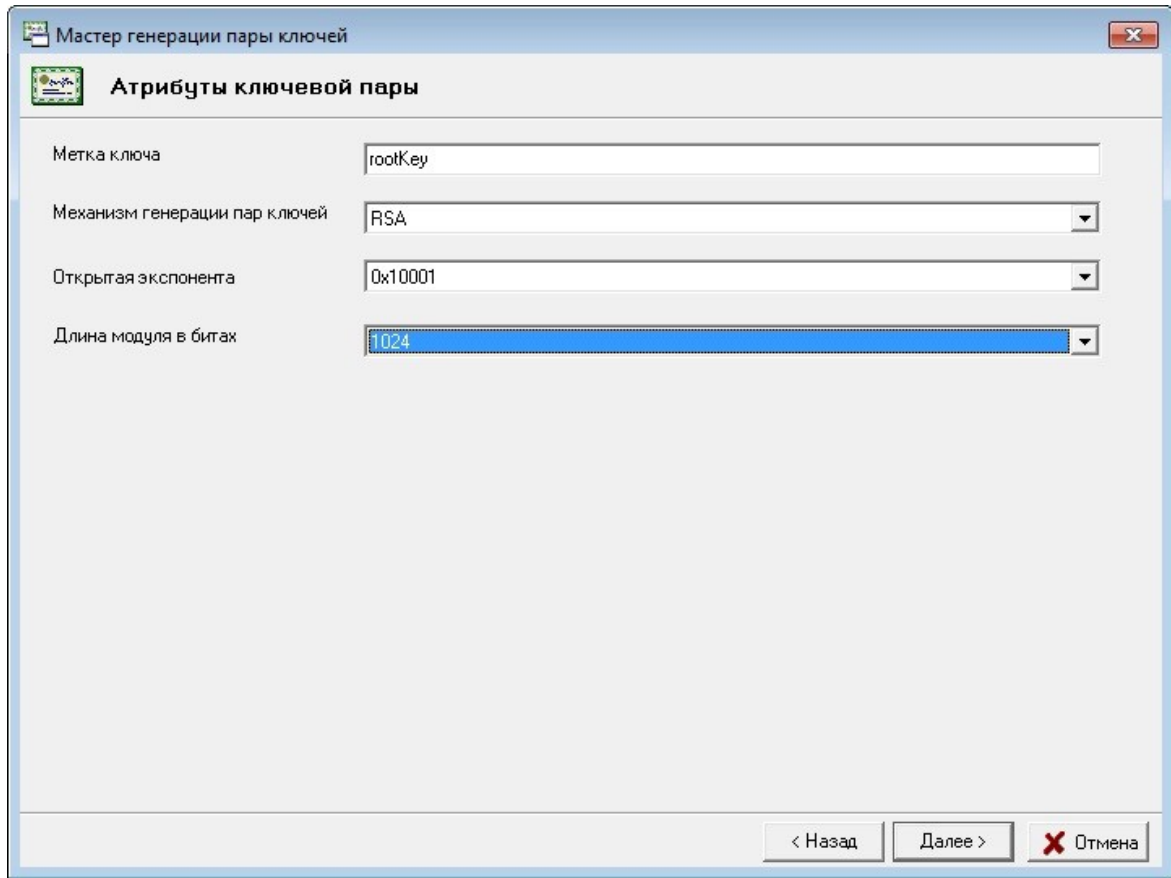
Малюнок 5. Вибір генерації пари ключів



Малюнок 6. Вибір атрибутів ключа

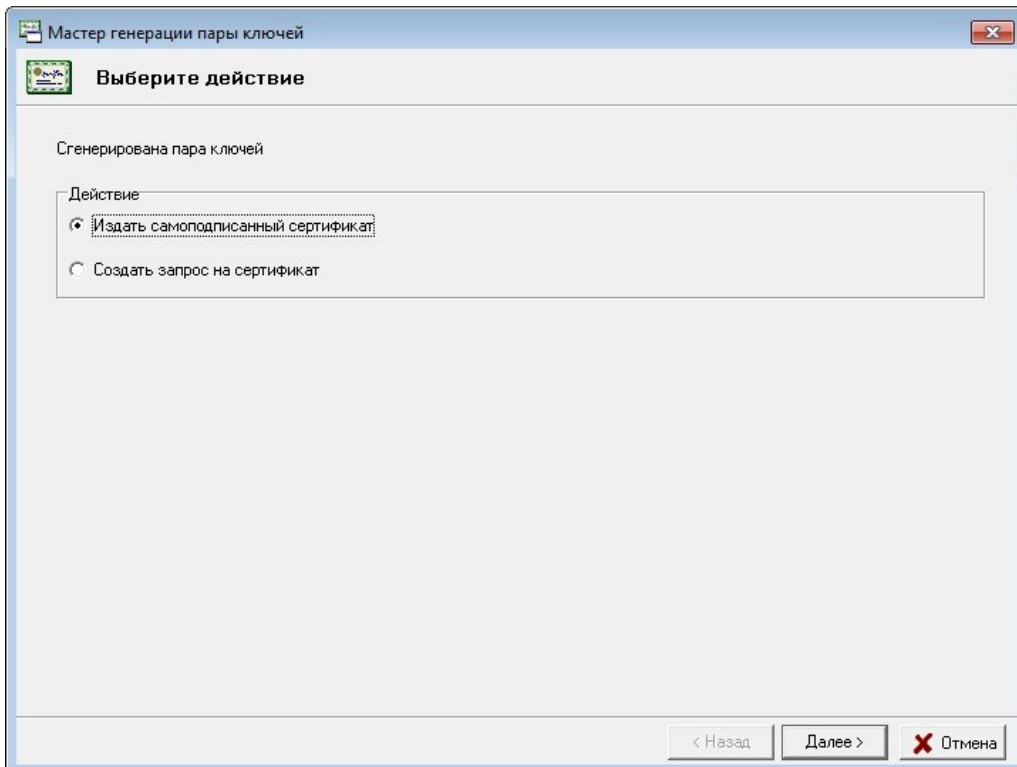
Генерація ключів доступна у двох режимах (див. Малюнок 7):

- ДСТУ 4145-2002
- RSA



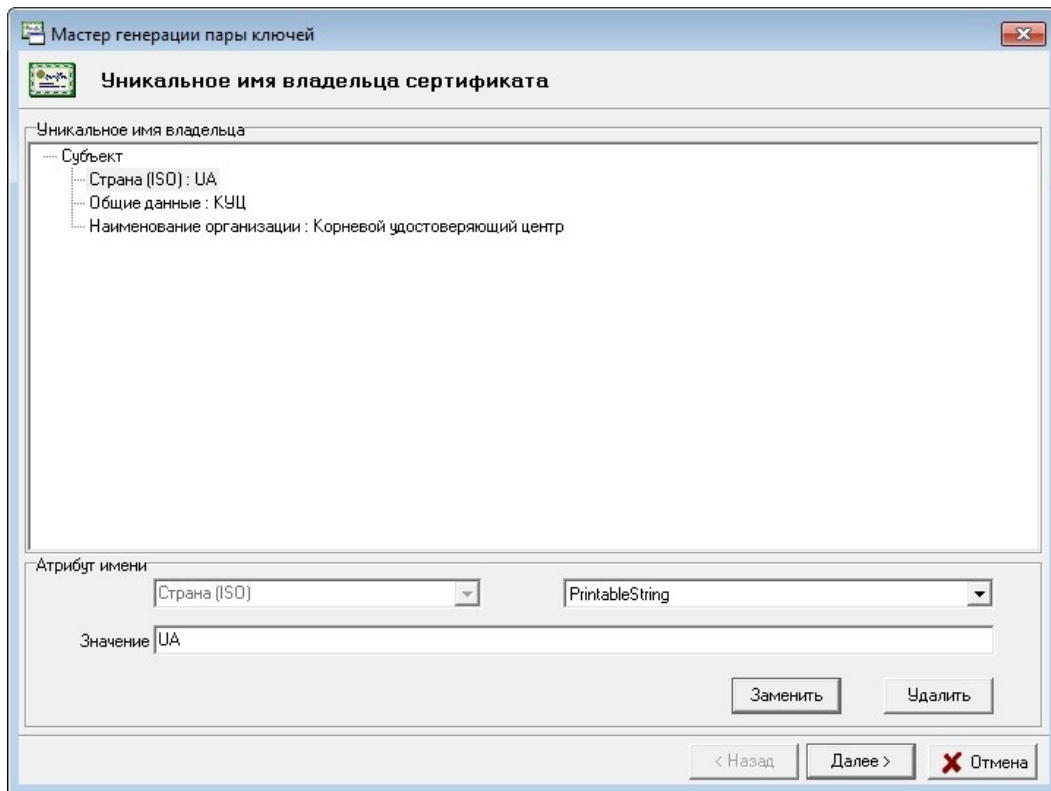
Малюнок 7. Вибір атрибутів ключової пари

Після створення ключа можна вибрати: чи видавати самопідписаний сертифікат або запит на сертифікат до вищестоящого ЗЦ (див. Малюнок 8).



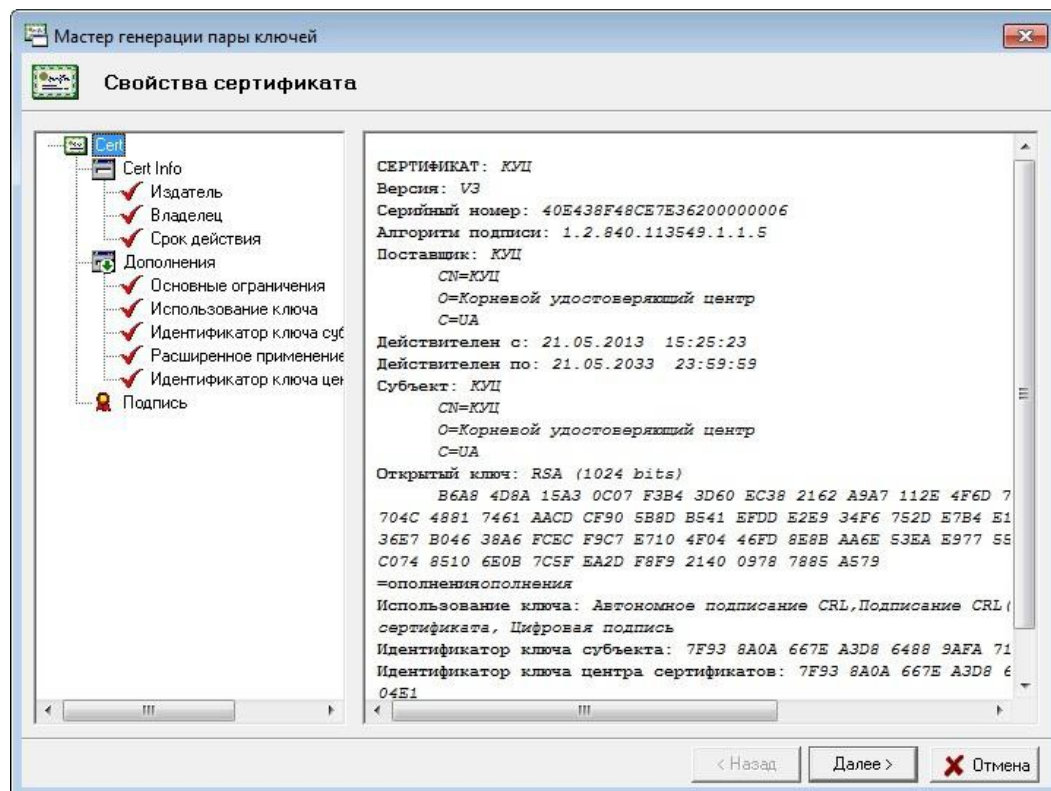
Малюнок 8. Вікно вибору дій

Вікно заповнення атрибутів сертифіката дозволяє задати значення полям майбутнього сертифікату (див. Малюнок 9).



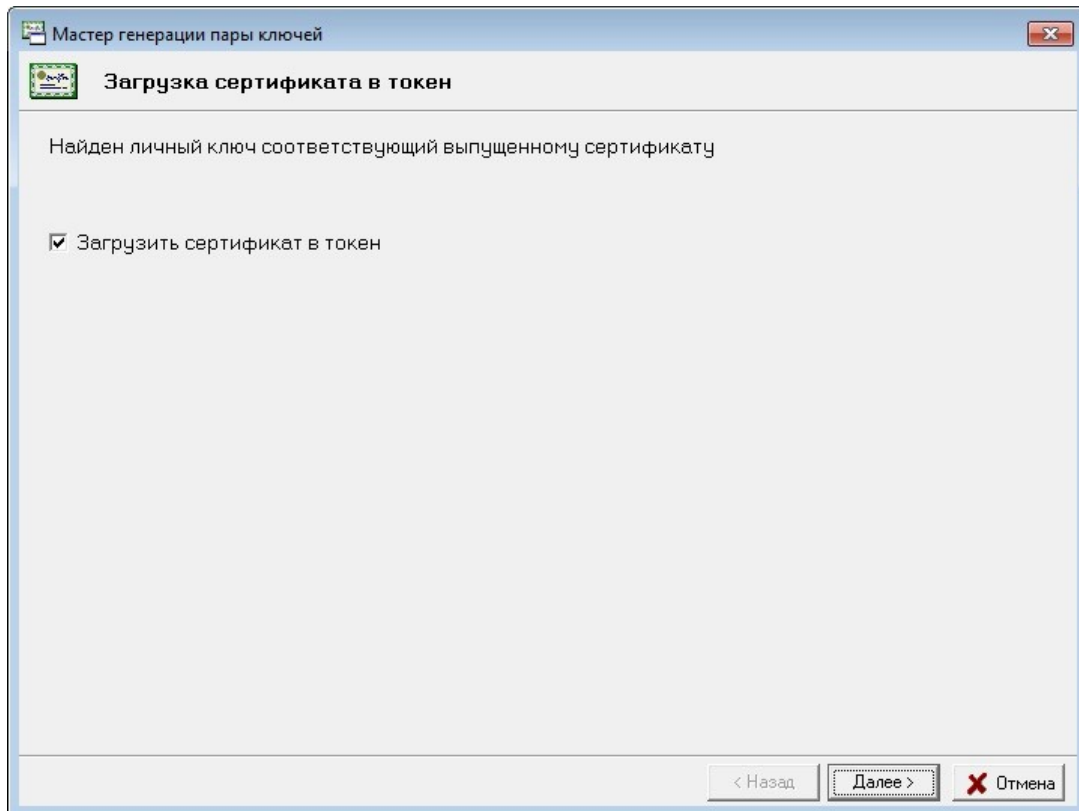
Малюнок 9. Вікно заповнення атрибутів сертифікату

Другий екран майстра дозволяє переглянути і відредагувати інші атрибути майбутнього сертифікату (див. Малюнок 10).



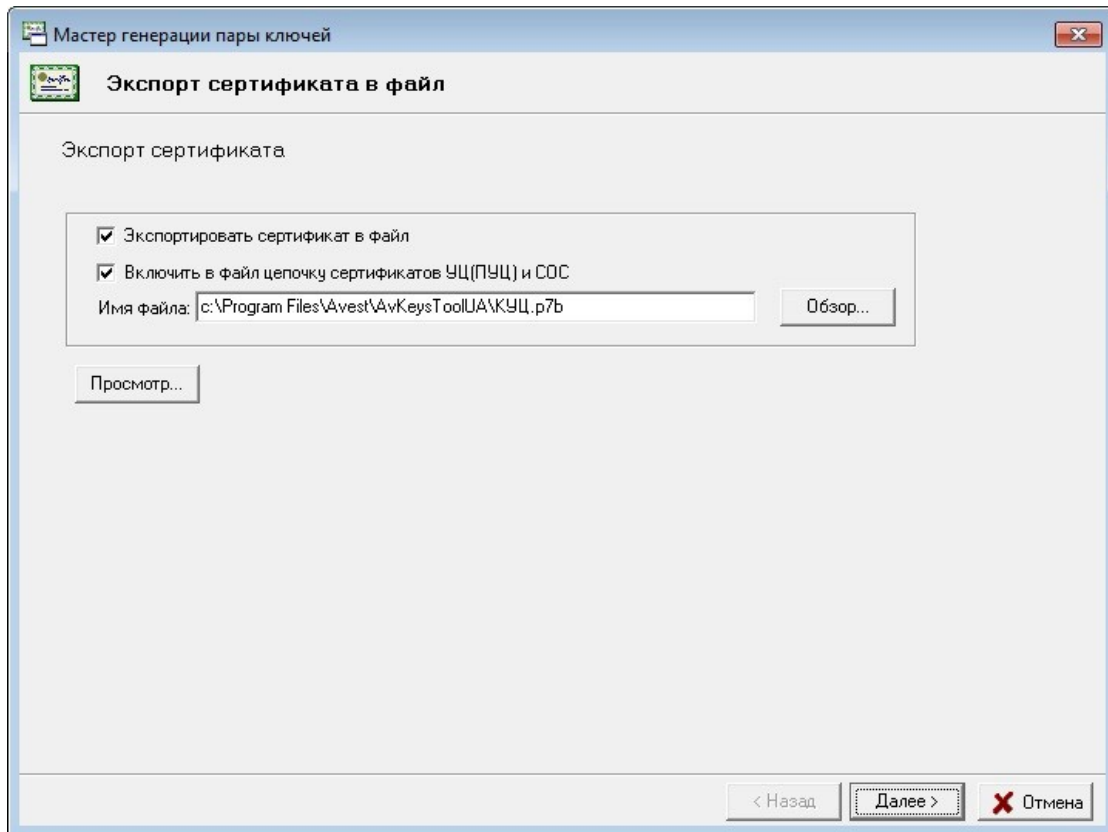
Малюнок 10. Перегляд властивостей сертифікату

На наступному кроці програма запропонує завантажити сертифікат у токен (див.Малюнок 11).

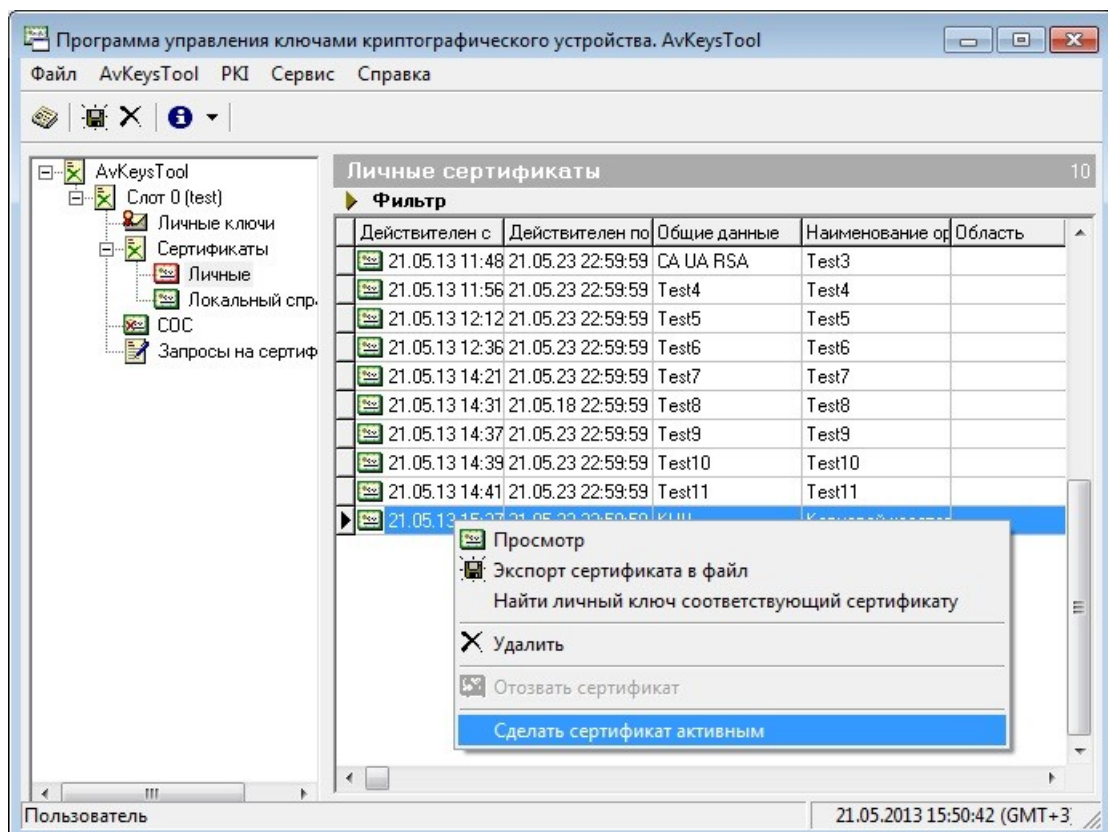


Малюнок 11. Завантаження сертифікатів у токен

Отримані сертифікати можна експортувати у вигляді файлу (див. Малюнок 12).



Для того щоб з отриманим сертифікатом можна було працювати, його потрібно зробити активним. Для цього потрібно викликати контекстне меню сертифікату і вибрати там пункт «Зробити сертифікат активним» (див. Малюнок 13).



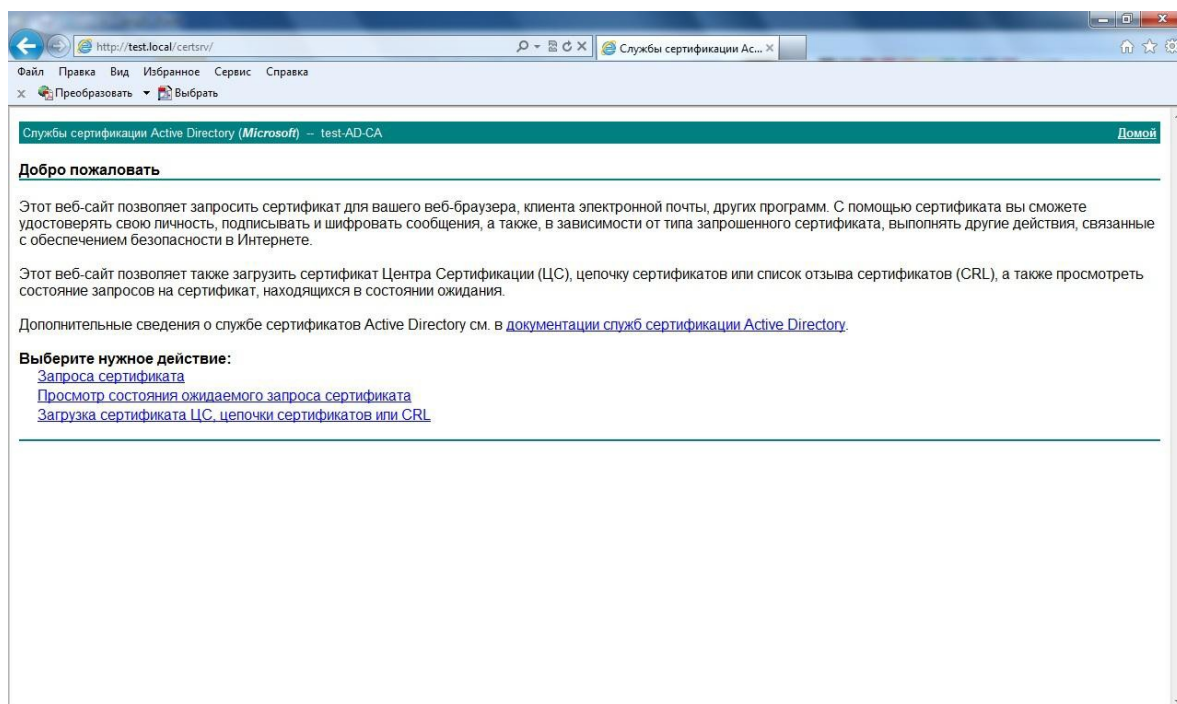
Після цього активний сертифікат отримує можливість через головне меню «РКІ» випускати СВС: меню «РКІ» - «Випустити черговий СВС» і обробляти запити на сертифікат: меню «РКІ» - «Обробити запит на сертифікат». Запити на сертифікат повинні мати розширення * .req, * .b64.

Логон за допомогою смарт-карт в клієнт-серверній архітектурі

Для успішного логону до домену за допомогою AvestKey необхідно згенерувати запит і отримати на підставі його в засвідчувальному центрі сертифікат.

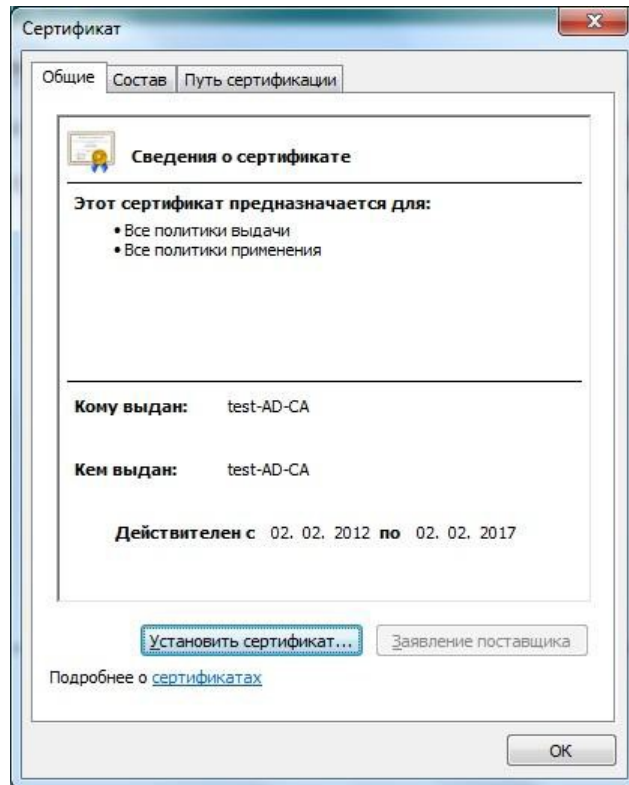
Для генерації запиту необхідно мати обліковий запис в домені. Порядок дій::

- авторизуватися в домені під обліковим записом користувача;
- відкрити через Internet Explorer веб-інтерфейсу Центру сертифікації <http://machine-name/certsrv>, де *machine-name* необхідно замінити ім'ям того комп'ютера, на якому працює Центр сертифікації (див. Малюнок 14);



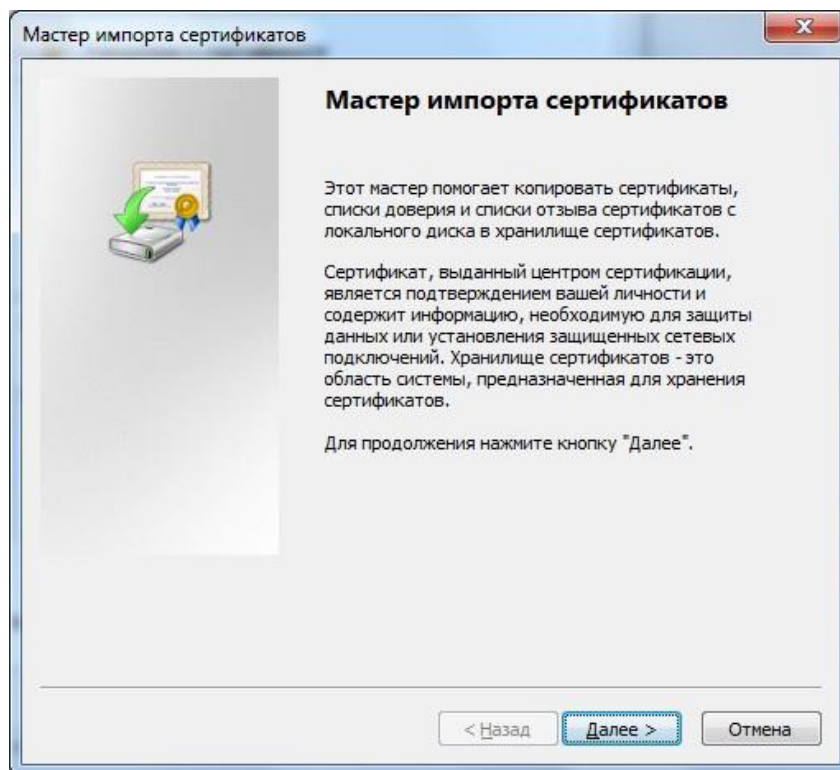
Малюнок 14. Веб-інтерфейс центру сертифікації

- у вікні запиту облікових даних для авторизації необхідно ввести дані користувача, для якого необхідно отримати сертифікат;
- у вікні вибрати пункт «Завантаження сертифікату ЦС», ланцюги сертифікатів або CRL». Відкрити завантажений файл та натиснути: Встановити сертифікат (див. Малюнок 15).

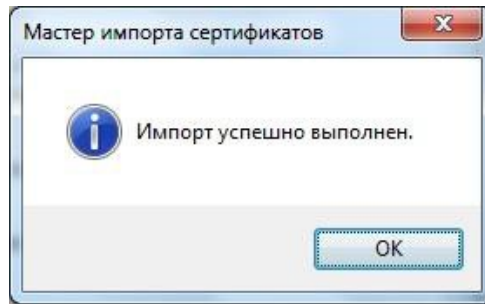


Малюнок 15. Сертифікат ЗЦ

- провести всі кроки, які відкриваються «Майстер імпорту сертифікатів». Результатом його роботи має бути повідомлення про успішний імпорт (див. Малюнок 16, Малюнок 17);

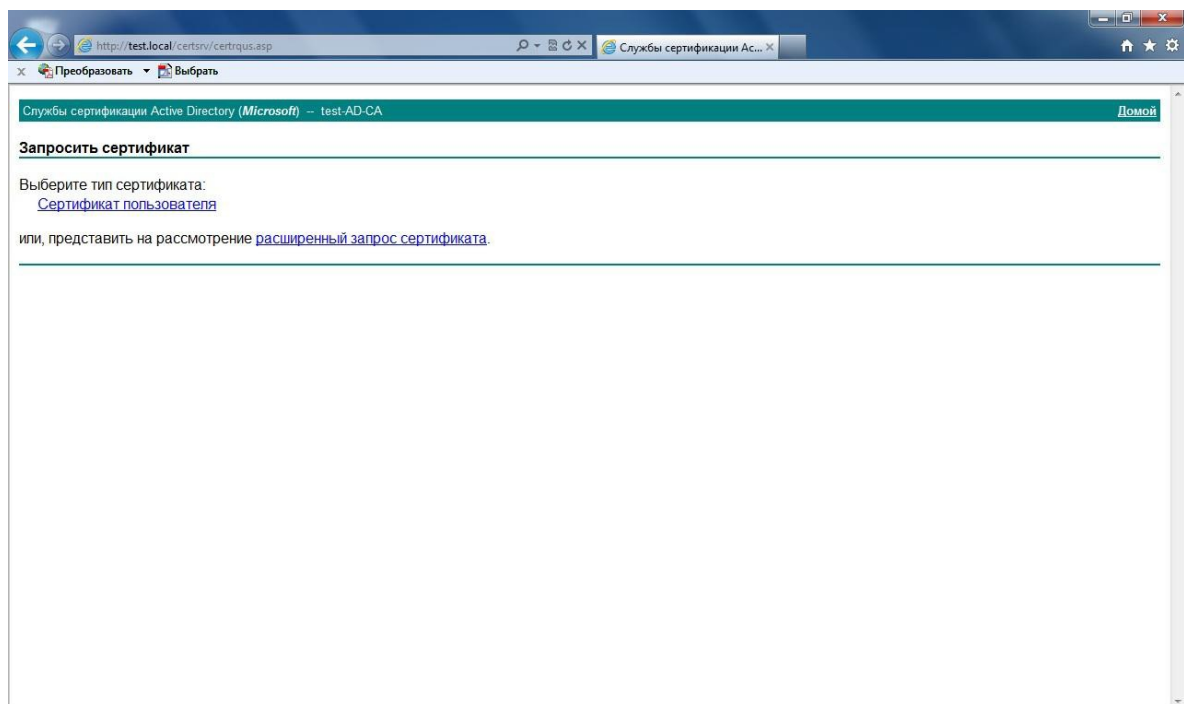


Малюнок 16 Майстер імпорту сертифікатів

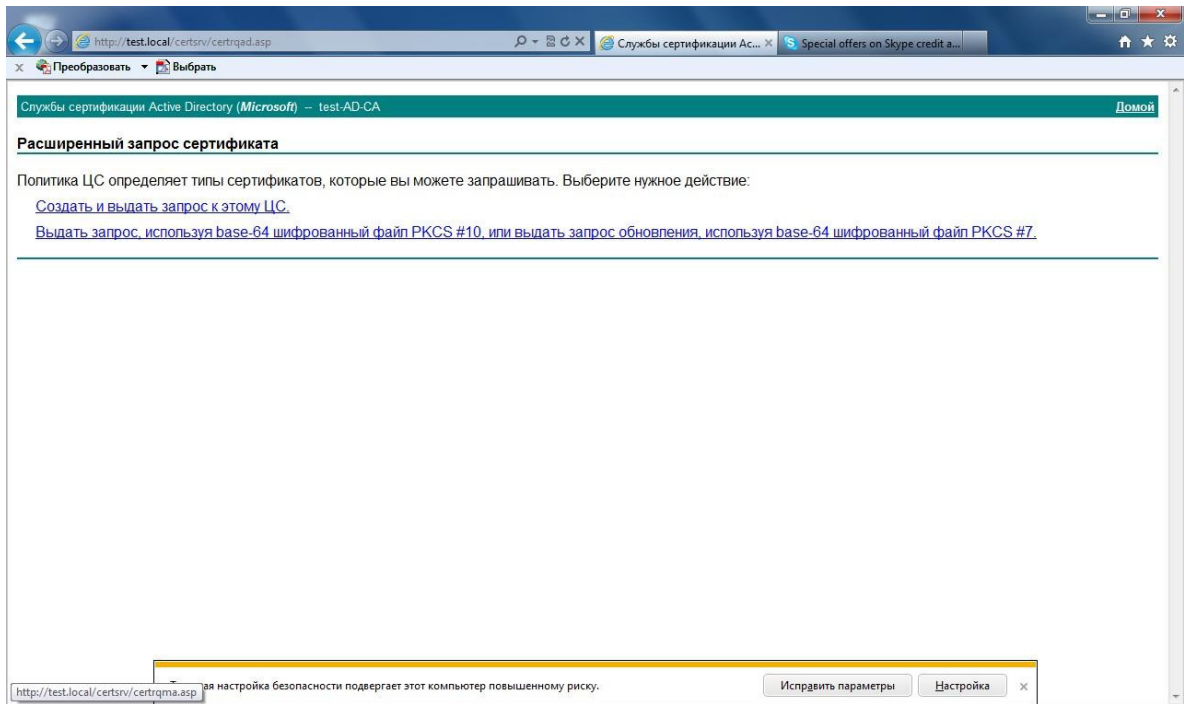


Малюнок 17. Вікно завершення процедури імпорту

- повернутися на головну сторінку служби сертифікатів та вибрати пункт «Запит сертифікату» (див. Малюнок 14). Далі у вікні вибрати «Розширений запит сертифікату» (див. Малюнок 18), потім – «Створити та видати запит до цього ЦС» (див. Малюнок 19).



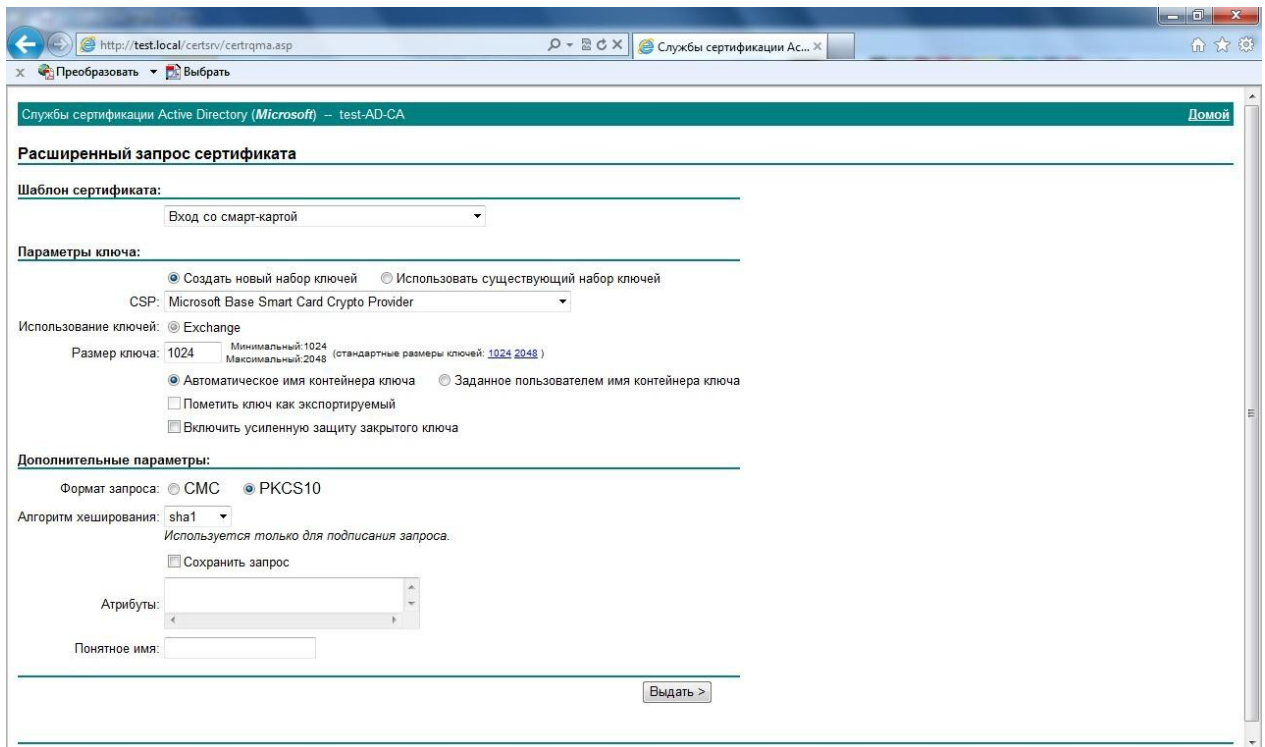
Малюнок 18. Вікно створення запиту на сертифікат



Малюнок 19. Вибір розширеного запиту сертифікату

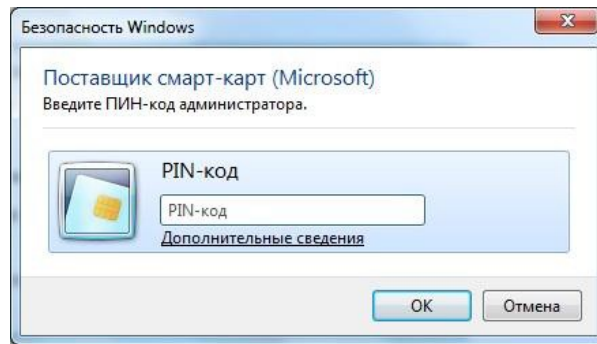
- Вікно розширеного запиту сертифікату заповнити за зразком, як показано на малюнку 1 і натиснути «Видати» (див. Малюнок 20);

Важливо: В полі «Шаблон сертифікату» необхідно вибрати пункт «Вхід зі смарт-картою». У розділі «Параметри ключа», в полі CSP необхідно вибрати пункт «Microsoft Base Smart Card Crypto Provider», пункті «Формат запиту» вказати PKCS10.



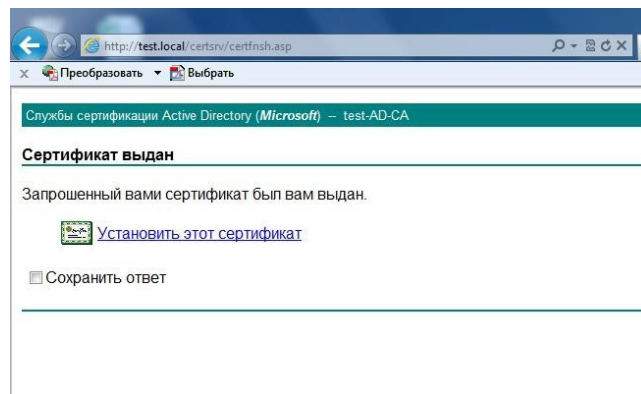
Малюнок 20. Заповнення запиту

- у вікні з пропозицією введення PIN-коду необхідно ввести пароль користувача (див. Малюнок 21);



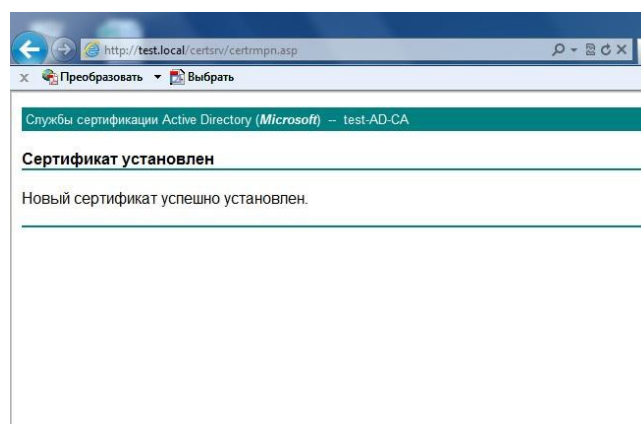
Малюнок 21. Запит вводу PIN-коду

- на сторінці центру сертифікації з'явиться пропозиція установити отриманий сертифікат. Зробити установку сертифікату (див. Малюнок 22);



Малюнок 22. Запит установки отриманого сертифікату

- далі відобразиться інформація про успішну установку сертифікату (див. Малюнок 23);



Малюнок 23. Повідомлення про успішну установку сертифікату

- Зробити вихід із операційної системи.

У вікні вибору користувачів з'явиться вікно з пропозицією входу по смарт-карті для даного користувача. Після введення PIN-коду користувача авторизація проходить успішно.