

Інструкція по генерації ключів на носії ключової інформації ТОВ «Автор» **(токени чи смарт-картки)**

1. Опис ПЗ в комплекті генерації (архів *Avtor_NKI.zip*)

Init337UM – утиліта первинної ініціалізації токенів

UmCA_Setup – інсталятор ПЗ генерації ключів

P11KeyUtil – утиліта для імпорту на токен ключових даних AnyConnect (використовується, якщо ваша установа працює в СДО «Клієнт Казначейства – Казначейство»)

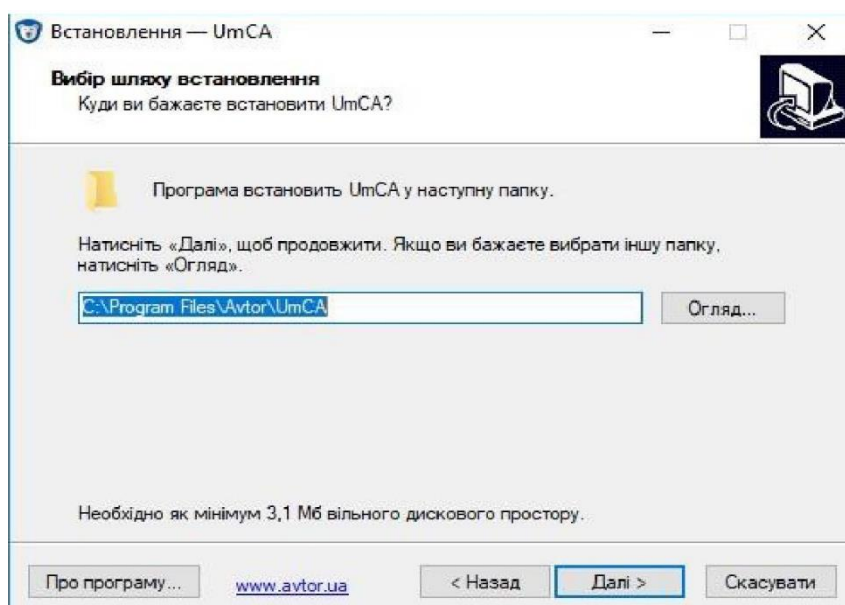
2. Підготовка до роботи – встановлення ПЗ генерації ключів UmCA

2.1. Системні вимоги

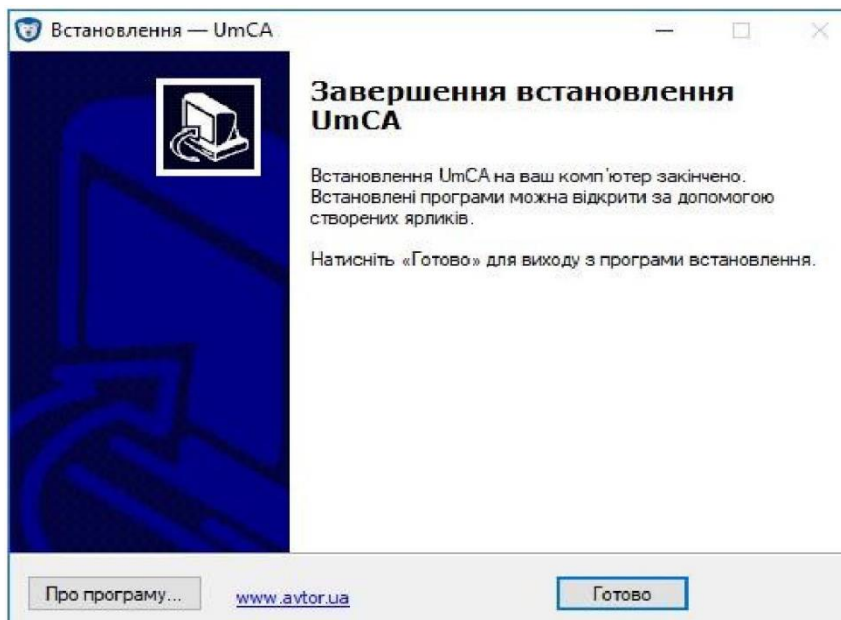
Використання ПЗ можливе в системах Windows 7 з пакетом оновлення SP1 (та встановленим .NET Framework не нижче версії 4.5.2), Windows 8.1 та Windows 10.

2.2. Порядок встановлення

Запустити *UmCA_Setup.exe* та у вікні, що з'явиться, обрати мову для подальшої роботи з Майстром встановлення, підтвердивши вибір кнопкою «ОК». Відкриється стартове вікно Майстра встановлення ПЗ. Натиснути «Далі» для продовження на цьому кроці і наступних, обрати шлях встановлення ПЗ.



На наступних кроках обрати папку в меню «Пуск» для створення ярлика програми та за необхідності, встановити відмітку створення ярлика на Робочому столі. Перевірити обрані налаштування та натиснути «Встановити» для початку процесу встановлення. Успішне завершення встановлення ПЗ виведе вікно «Завершення встановлення».

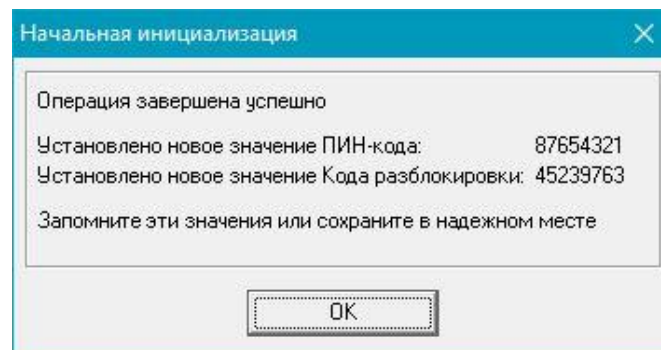
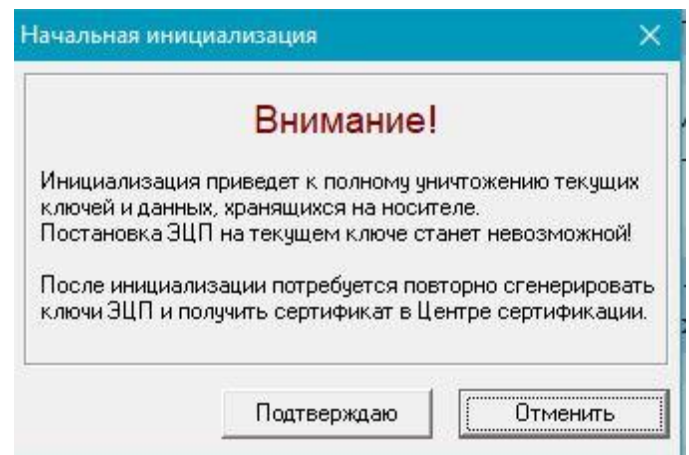
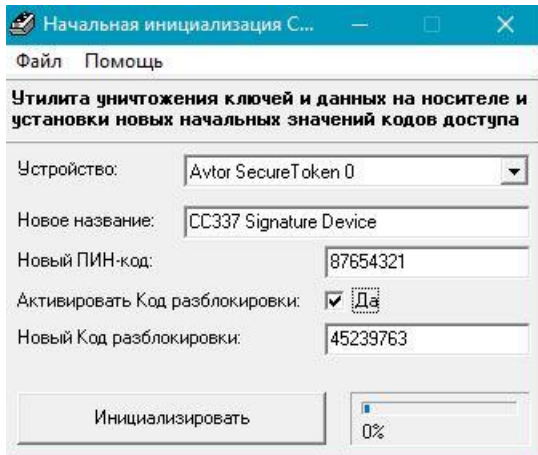


3. Підготовка до роботи – ініціалізація токена

Увага! Під час виконання ініціалізації знищуються будь-які ключові дані, що були попередньо записані на носій ключової інформації (далі – НКІ).

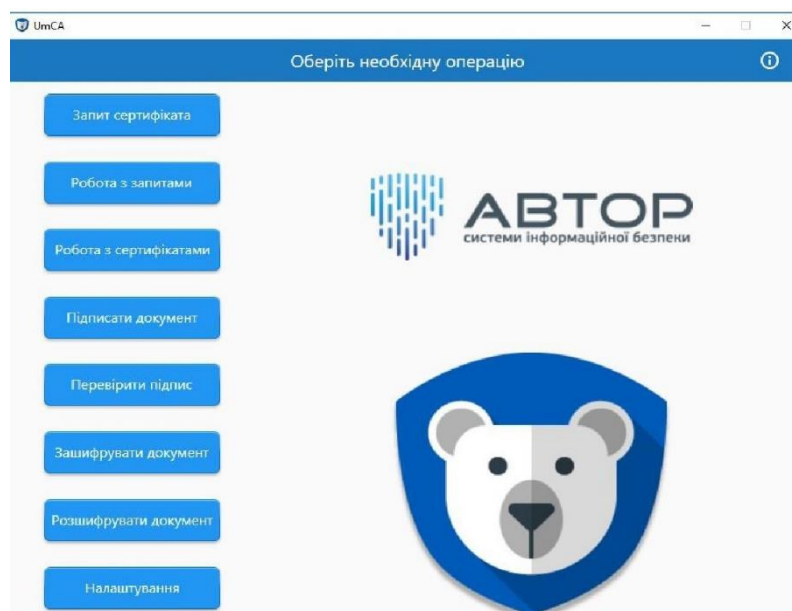
Запустити утиліту *Init337UM*

- в поле «Название устройства» можна, за бажанням, вписати латинськими літерами нову назву-мітку пристрою (використовується для зручності та не є обов'язковим);
- в поле «Новый ПИН-код» вписати надійний цифровий пароль (максимум 8 цифр);
- відмітити «Активировать код разблокировки» та вписати в полі «Новый код разблокировки» зручний код розблокування токена, який легко вам запам'ятати (не може співпадати з ПИН-кодом, використовується для розблокування токена через 7 невдалих спроб вводу ПИН-коду);
- натиснути кнопку «Инициализировать»



4. Генерація пари ключів на НКІ та отримання електронних запитів на сертифікати

Після підготовки НКІ до роботи (п.3) запустити встановлене ПЗ *UmCA* та натиснути кнопку «Запит сертифіката»



У вікні буде відображено інтерфейс, в якому необхідно:

- обрати призначення сертифіката – для підпису (запит на сертифікат шифрування буде запропоновано згенерувати автоматично після генерації запиту на підпис – генерувати запит шифрування обов’язково, для цього слід встановити позначку **«Рекомендувати генерацію другого сертифіката»** у Налаштуваннях);
- обрати власника сертифіката: фізична особа, що є представником юридичної особи (у разі формування сертифіката підписувача) або юридична особа (у разі формування сертифіката печатки установи);
- обрати носій для запису сертифіката: тільки **токен** (підключений до ПК апаратний носій, що може бути у вигляді токена або смарт-карти);
- заповнити дані запиту (поля відображаються в залежності від власника сертифікату, поля запиту на сертифікат, позначені зірочкою (*), є обов’язковими до заповнення).

Примітка. Якщо апаратний носій було під’єднано в процесі роботи з даним вікном, натисніть кнопку «Оновити» для актуалізації доступних носіїв.

У випадку, якщо був обраний пункт **«Фізична особа – представник юридичної особи»**, то в блоці опцій «Дані сертифіката» з’являться поля для заповнення.

Обов’язковими для заповнення є поля:

- Повне ім’я
- Прізвище
- Ім’я, по батькові
- Країна (незмінне значення UA)
- Область (обрати зі списку «Херсонська»)
- Місто (із скороченим зазначенням типу населеного пункту згідно дод.1 на формування сертифікатів – м., смт, с., сел. чи хут.)
- Організація
- Код ЄДРПОУ
- ІНН

Зверніть увагу!

- в полі **«Повне ім’я»** вказується прізвище, ім’я, по батькові підписувача без скорочень;
- в полі **«Організація»** вказується повна назва організації, згідно установчих документів (або, якщо довжина повної назви із врахуванням всіх знаків пунктуації перевищує 64 символи, вказується скорочена назва згідно установчих документів, а у разі її відсутності – варіант скороченої назви згідно наданого супровідного листа);
- в полі **«ІНН»** вказується реєстраційний номер облікової картки платника податків (якщо через релігійні переконання підписувач відмовився від отримання ІНН, до цього поля вписується серія в латинській транслітерації та номер паспорта – наприклад, MR012034);
- в полі **«Номер у ЄДДР»** вказується унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності).

Приклад коректно заповненої форми для формування запиту на сертифікат підписувача:

UmCA

Генерація сертифіката

Запит сертифіката

Робота з запитами

Робота з сертифікатами

Підписати документ

Перевірити підпис

Зашифрувати документ

Розшифрувати документ

Налаштування

Призначення сертифіката для: підпису

Власник сертифіката: Фізична особа - представник юридичної особи

Носій сертифіката:

☒ Токен: Avtor SecureToken 0
 ☐ Рfх-контейнер:

Дані сертифіката

Повне ім'я* Іванов Іван Іванович

Прізвище* Іванов

Ім'я, по батькові* Іван Іванович

Країна* UA

Область* Херсонська

Місто* м. Херсон

Організація* Дошкільний навчальний заклад №99 "Червона калина"

Підрозділ

ЄДРПОУ* 01020304

Посада

ІНН* 0123456789

Електронна адреса

Серійний номер

Номер у ЄДДР 19850515-00034

☐ Печатка

Оновити

Створити

Зберегти запит

У випадку, якщо був обраний пункт «**Юридична особа**», то в блоці опцій «Дані сертифіката» з'являться відповідні поля для заповнення.

Обов'язковими для заповнення є поля:

- Повне ім'я
- Країна (стандартно заповнюється – UA)
- Область (обрати зі списку «Херсонська»)
- Місто (із скороченим зазначенням типу населеного пункту згідно дод.1 на формування сертифікатів – м., смт, с., сел. чи хут.)
- Організація
- Код ЄДРПОУ
- Зазначення, що ключ буде використовуватись як печатка

Зверніть увагу!

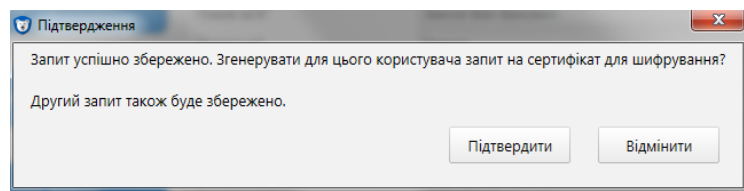
В полях «**Повне ім'я**» та «**Організація**» вказується повна назва організації, згідно установчих документів (або, якщо довжина повної назви із врахуванням всіх знаків пунктуації перевищує 64 символи, вказується офіційна скорочена назва, а у разі її відсутності – варіант скороченої назви згідно наданого супровідного листа).

Приклад коректно заповненої форми для формування запиту на сертифікат печатки установи:

У разі коректного заповнення полів, після натискання кнопки «Зберегти запит» програма запропонує ввести ПІН-код для роботи із НКІ, що необхідно підтвердити натисненням клавіші «ОК». Для збереження файлу запиту (формат файлу – *.p10) необхідно вказати шлях, де буде збережено зазначений файл (в імені файлу запиту **не повинно бути спецсимволів**).

У разі помилок при заповненні форми на екран буде виведено відповідне повідомлення, при цьому запит не буде сформовано. Необхідно внести зміни відповідно до підказок і повторити спробу.

Після успішного завершення операції формування запиту на екран буде виведено відповідне повідомлення та користувачу буде запропоновано згенерувати запит для сертифіката шифрування – натиснути «Підтвердити», ще раз ввести ПІН-код та зберегти файл запиту.



Запити на сертифікати необхідно записати на флеш-носії і надати в ВПР разом із документами, що визначені Регламентом роботи кваліфікованого надавача електронних довірчих послуг Державної казначейської служби України, та обов'язково внести імена цих файлів запитів до відповідних полів дод.1 заяви про формування сертифікатів.

Для зручності файли запитів можна перейменувати за шаблоном:

Печатка_КЕП.p10 та Печатка_Ш.p10 – для запитів підпису і шифрування сертифікатів печатки; Прізвище_КЕП.p10 та Прізвище_Ш.p10 – для запитів підпису і шифрування сертифікатів підписувача (див. приклади).

Запити на формування сертифіката (за наявності)			
Печатка_КЕП.p10		Печатка_Ш.p10	
(вказати назву файлу запиту)		(вказати назву файлу запиту)	

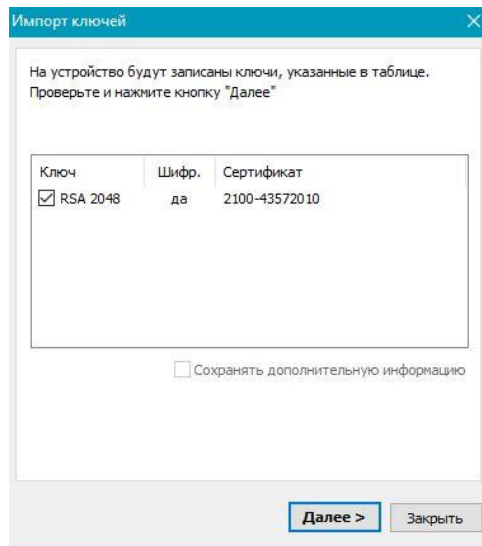
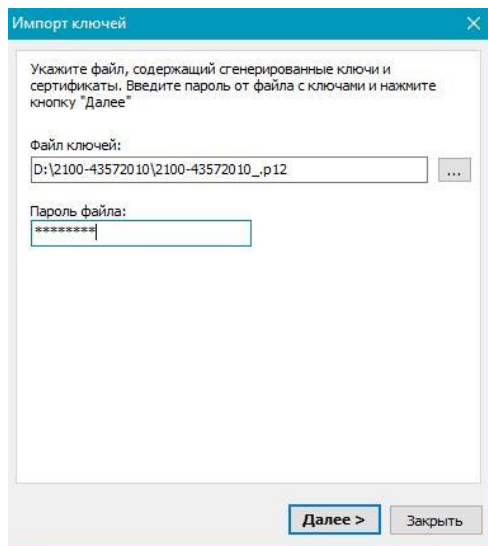
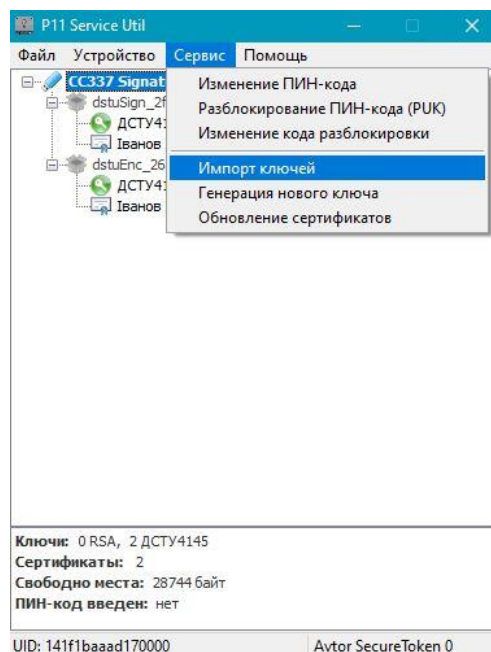
Запити на формування сертифіката (за наявності)			
Іванов_КЕП	.p10	Іванов_III	.p10
(вказати назву файлу запиту)		(вказати назву файлу запиту)	

5. Імпорт отриманих від АЦСК сертифікатів на НКІ

Після надання до АЦСК або ВПР файлів запитів та подальшого отримання відповідних сертифікатів (з сайту <http://ca.treasury.gov.ua> в розділі «Пошук сертифікатів»), в ПЗ UmCA натиснути кнопку «Робота із запитами», потім «Перевірити статус запитів» – будуть відображені наявні на НКІ запити сертифікатів підпису та шифрування, після чого натиснути «Занести на носій» та обрати шлях до збережених сертифікатів.

6. Імпорт ключових даних AnyConnect (тільки для тих НКІ, які працюють безпосередньо в СДО «Клієнт Казначейства – Казначейство»)

- 1) Під'єднати токен, на який потрібно імпортувати ключові дані AnyConnect до комп'ютера та запустити сервісну утиліту *P11KeyUtil*, обрати серед меню «Устройство» та натиснути в ньому на знайдений токен.
- 2) Після відображення даних на токені буде доступне меню «Сервис» – в ньому обрати «Импорт ключей» та ввести ПИН-код.
- 3) В наступному вікні в поле «Файл ключей» обрати шлях до криптоконтейнера *.p12, а в поле «Пароль файла» скопіювати/внести пароль імпорту, що надається в текстовому файлі разом із криптоконтейнером та натиснути «Далее», утиліта покаже інформацію про тип ключа, що імпортується до НКІ – натиснути ще раз «Далее» та після повідомлення про успішний імпорт – «Заккрыть» (в прикладі використано AnyConnect установи з ЄДРПОУ 43572010).



Ключові дані AnyConnect для самостійного імпорту на НКІ можна отримати в ВІР, який надає електронні довірчі послуги вашій установі.