**Інструкція з віддаленої генерації КЕП на захищеному носії AvestKEY.**

## 1. Налаштування роботи захищеного носія на робочому ПК

Для налаштування роботи захищеного носія **AvestKey** на робочому ПК завантажте драйвер за посиланням та встановіть його (**ВАЖЛИВО! Спочатку встановлюється драйвер, після цього можна встановлювати носій у USB порт ПК)**:

https://avest.com.ua/wp-content/uploads/2021/06/ustanovchi-dravery-dlya-vsih-operaczijnyh-system.zip

ПЗ AvKeysTool для управління захищеним носієм **AvestKey** знаходиться за посиланням:

https://avest.com.ua/wp-content/uploads/2021/06/avestkeytools.zip

Інструкція з роботи ПЗ AvKeysTool знаходиться за посиланням:

https://avest.com.ua/wp-content/uploads/2021/02/avkeystool_ukr.pdf

В подальшому ПЗ AvKeysTool Вам знадобиться для зміни стандартного паролю (пін коду) носія на власний пароль (стандартний пароль доступу до носія 12345678).

## 2. Віддалена генерація КЕП за допомогою сервісів ДПС

2.1. Для віддаленої генерації КЕП за допомогою сервісів ДПС перейдіть за посиланням: https://acskidd.gov.ua – тут Ви знайдете всю необхідну інформацію по отриманню КЕП

2.2. Отримання електронних довірчих послуг, у тому числі для програмних РРО знаходиться за посиланням: https://acskidd.gov.ua/etrusted-services

2.3. Переходите на вкладку «програмне забезпечення»

2.4. ПЗ Засіб кваліфікованого електронного підпису чи печатки - "ІІТ Користувач ЦСК-1" за посиланням: «Докладніше»

2.5. Завантажуєте Інсталяційний пакет "ІІТ Користувач ЦСК-1.3.1": https://acskidd.gov.ua/download/INSTAL/EUInstall.zip та встановлюєте на робочий ПК. **Важливо!!! При встановлені НЕ ВИБИРАТИ встановлення драйверів Алмаз, Кристал**

2.6. Настанова користувача "ІІТ Користувач ЦСК-1.3.1" за посиланням: https://acskidd.gov.ua/download/manual/EU13OManualDPS.zip

2.7. Налаштовуєте ІІТ Користувач ЦСК-1.3.1 – опис в Настанова користувача "ІІТ Користувач ЦСК-1.3.1" (стор. 17-19)

2.8. Переходите на вкладку «Повторне (дистанційне) формування сертифікатів за електронним запитом»

2.9. Завантажте криптоплагін за посиланням та встановіть його на робочий ПК:

– ОС Microsoft Windows - http://iit.com.ua/download/productfiles/EUSignWebInstall.exe

– ОС Linux (Debian\Ubuntu) x32 - http://iit.com.ua/download/productfiles/euswi.deb

– ОС Linux (Debian\Ubuntu) x64 - http://iit.com.ua/download/productfiles/euswi.64.deb

– ОС Linux (RHEL\CentOS\Fedora) x32 - http://iit.com.ua/download/productfiles/euswi.rpm

– ОС Linux (RHEL\CentOS\Fedora) x64 - http://iit.com.ua/download/productfiles/euswi.64.rpm

– ОС Linux x32 - http://iit.com.ua/download/productfiles/euswi.tar

– ОС Linux x64 - http://iit.com.ua/download/productfiles/euswi.64.tar

– ОС Apple Mac OS X - http://iit.com.ua/download/productfiles/EUSignWebInstall.pkg

Додатково, у випадку, якщо ОС або браузер не підтримує роботу з агентом підпису необхідно встановити веб-розширення для браузерів:

– Google Chrome - https://chrome.google.com/webstore/detail/%D1%96%D1%96%D1%82-%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87- %D1%86%D1%81%D0%BA-1-%D0%B1%D1%96%D0%B1%D0%BB/jffafkigfgmjafhpkoibhfefeaebmccg?utm_source=chrome-app- launcher-info-dialog

– Opera - https://addons.opera.com/uk/extensions/details/iit-end-user-ca-1-sign-web-extension/?display=uk

– Mozilla Firefox - https://eu.iit.com.ua/download/productfiles/eusw@iit.com.ua.xpi

**(ВАЖЛИВО! Відключіть перед завантаженням антивірус та програми, що блокують вікна, які вспливають)**
**Інтсрукція по роботі, налаштуванню та встановленю криптоплагіну знаходиться за посиланням:**
https://iit.com.ua/download/productfiles/EUSignWebOManual.pdf

2.10. Вибираєте пункт «Файловий носій» та вибираєте діючий ключ у файлі
2.11. Вводите пароль до файлу за КЕП та нажимаєте «Зчитати»
2.12. На наступному кроці підписуєте Договір
2.13. На наступному кроці вибираєте захищений носій AvestKey, якщо криптоплагін був встановлений на ПК коректно, система автоматично виявить захищений носій AvestKey.
2.14. Вводите пароль до носія AvestKey (стандартний пароль: 12345678). Після цього можна буде замінити стандартний пароль на власний індивідуальний в ПЗ AvKeysTool (див. п. 1 цієї інструкції)
2.15. На останньому кроці будуть сформовані власні сертифікати, їх потрібно зберегти у директорію на диску C:\My Certificates and CRLs 13
2.16. Для завантаження всіх інших потрібних сертифікатів запустіть «IIT Користувач ЦСК-1.3.1» та в меню Сертифікати та СВС оберіть підпункт «Отримати з ЦСК» стор. 15 Настанови користувача "IIT Користувач ЦСК-1.3.1"
2.17. При зчитуванні КЕП з захищеного носія треба обрати носій зі списку з назвою е.ключ та/або смарт-карта AVEST (pkcs#11) (ВАЖЛИВО! Обирайте саме цей пункт!) та ввести пароль до захищеного носія AvestKey (якщо Ви ще не змінювали пароль у ПЗ AvKeysTool, то стандартний пароль: 12345678)

**Користуйтеся захищеним носієм AvestKey зі згенерованим КЕП**

## 3. Віддалена генерація КЕП за допомогою M.E.Doc

3.1. Для налаштування роботи M.E.Doc з захищеним носієм AvestKey Вам потрібно завантажити бібліотеку, відповідно до Вашої операційної системи відповідної розрядності x32 або x64. Для цього перейдіть за посиланням: https://avest.com.ua/wp-content/uploads/2021/06/lib.zip,
бібліотека знаходиться у папці \lib з назвою avcryptokinxt.dll

3.2. Додайте (скопіюйте) бібліотеку відповідної розрядності в директорію \32 або \64 кореневого каталогу встановленого екземпляру програми M.E.DOC

3.3. В файлі UniCryptD.ini, що знаходиться в директоріях \32 та/або \64 кореневого каталогу, додати запис:

Library[наступний порядковий номер]=[назва бібліотеки]
Name[наступний порядковий номер]=AVEST01
Наприклад:
Library12=avcryptokinxt.dll
Name12=AVEST01
При мережевому варіанті роботи дані операції потрібно зробити на робочій станції та сервері.

3.4. Перезапускаємо M.E.Doc

3.5. Якщо M.E.Doc не знаходить захищений носій AvestKey, перезапускаємо служби M.E.Doc в ручному режимі

3.6. Можна генерувати КЕП на захищений носій, згідно Інструкцій M.E.Doc (наприклад: https://www.youtube.com/watch?v=kmWiZt8Kcm4 або https://medoc.ua/faq/jak-perevidati-sertifkati-kep-na-zahishhenij-nosj-bez-vdvduvannja-centru)

**Гарної роботи!!!**