Практична робота. ***Використання електронно-цифрового підпису***

Методичні вказівки

Використання новітніх ІТ-технологій дозволяє досягти істотного і швидкого зменшення непродуктивних витрат. Одним з важливих шляхів є перехід до без паперових технологій роботи з документами та впровадження безпечних технологій дистанційного надання послуг. Вирішення цього завдання тісно пов'язане з регулюванням використання електронного підпису в Україні.

Так, наприклад, з осені 2017 року в Україні відбувся початок видачі внутрішніх паспортів у вигляді ID-картки одразу з електронним цифровим підписом (ЕЦП), та впровадження MobileID (ЕЦП на SIM-картці).

Правовий статус електронного цифрового підпису в Україні визначається Законом України «Про електронний цифровий підпис». Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності визначається Кабінетом Міністрів України. Порядок застосування електронного підпису, у тому числі електронного цифрового підпису в банківській системі України та суб'єктами переказу коштів визначається Національним банком України.

Слід розрізняти поняття «електронний підпис» та «електронний цифровий підпис».

Під **електронним підписом (ЕП)** розуміються дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних.

Наприклад, електронним підписом є комбінація логіна і пароля, що вводяться користувачем при реєстрації в системі.

При підтвердженні здійснення банківського платежу в електронній формі, електронним підписом стане введення користувачем отриманого від банку перевірочного коду і підтвердження його введення натисканням клавіші Enter.

Під **електронним цифровим підписом (ЕЦП)** розуміється такий електронний підпис що був отриманий в результаті криптографічного перетворення набору електронних даних.

Електронний цифровий підпис дає змогу підтвердити цілісність підписаного з його допомогою документа та ідентифікувати підписувача.

Електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів. Укладення юридичними особами господарських угод в електронній формі з використанням сторонами ЕЦП є повністю правомірним.

У випадках, коли відповідно до законодавства необхідне засвідчення дійсності підпису на документах та відповідності копій документів оригіналам на електронний документ накладається ще один електронний цифровий підпис юридичної особи (наприклад, ЕЦП нотаріуса), спеціально призначений для таких цілей. Такий додатковий ЕЦП називається електронною печаткою.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Особистий ключ - параметр електронного цифрового підпису, доступний тільки підписувачу.

Відкритий ключ – параметр електронного цифрового підпису, доступний всім суб'єктам відносин у сфері використання електронного цифрового підпису.

Відкритий ключ електронного цифрового підпису використовується для перевірки електронного цифрового підпису.

У тих випадках, коли ЕЦП використовується для підпису зашифрованого документа, в цілях безпеки використовується дві пари ключів. Одна пара ключів використовується для шифрування документа (т.з. ключі для протоколу розподілу), а друга пара ключів - для накладення на документ електронного цифрового підпису.

Сертифікатом відкритого ключа є документ, який засвідчує чинність і належність відкритого ключа ЕЦП підписувачу. Сертифікати відкритих ключів можуть розповсюджуватися в електронній формі або у формі документа на папері.

Нотаріуси, державні реєстратори прав на нерухоме майно, державні реєстратори юридичних осіб, фізичних осіб - підприємців та громадських формувань повинні використовувати тільки **захищені носії особистих ключів** (наприклад, смарт-карти, електронні ключі, крипто модулі) що забезпечують захист записаних на нього даних від несанкціонованого доступу. Для кожного особистого ключа потрібен окремий носій.

Органи сертифікації:

Відповідно до Закону України «Про електронний цифровий підпис» в Україні існує п'ять видів органів, пов'язаних з сертифікацією ключів:

1. Центри сертифікації ключів (ЦСК).
2. Акредитовані центри сертифікації ключів (АЦСК).
3. Центральний засвідчувальний орган (ЦЗО).
4. Засвідчувальний центр органу виконавчої влади або іншого державного органу (ЗЦ)
5. Контролюючий орган (КО). Держспецзв’язок

Центром сертифікації ключів (ЦСК) може бути юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги електронного цифрового підпису та засвідчила свій відкритий ключ у центральному засвідчувальному органі (ЦЗО) або засвідчувальному центрі (ЗЦ).

Акредитованим центром сертифікації ключів (АЦСК) є Центр сертифікації ключів (ЦСК), акредитований відповідно «Порядку акредитації центру сертифікації ключів», що був затверджений постановою №903 Кабінету Міністрів України від 13 липня 2004 р. АЦСК повинен використовувати для надання послуг в сфері цифрового підпису лише надійні засоби ЕЦП, що мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації.

Центральний засвідчувальний орган (ЦЗО) видає посилені сертифікати ключів центрам сертифікації ключів (АЦСК) та засвідчувальним центрам (ЗЦ).

Центральний засвідчувальний орган визначається Кабінетом Міністрів України. Постановою Кабінету Міністрів України «Про затвердження Положення про центральний засвідчувальний орган» з жовтня 2011 року виконання функцій Центрального засвідчувального органу було покладено на **Міністерство юстиції України**.

Технічне та технологічне забезпечення виконання функцій центрального засвідчувального органу здійснюється державним підприємством «Інформаційний центр» Міністерства юстиції України, яке визначено адміністратором інформаційно-телекомунікаційної системи центрального засвідчувального органу.

Щорічну планову перевірку Центрального засвідчувального органу (ЦЗО) здійснила комісія у складі працівників Державної служби спеціального зв’язку та захисту інформації (ДССЗЗІ).

Засвідчувальний центр центрального органу виконавчої влади (ЗЦ) визначається Кабінетом Міністрів України для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи центрів сертифікації ключів (ГЦСК), які надають послуги електронного цифрового підпису цьому органу і підпорядкованим йому підприємствам, установам та організаціям.

Інші державні органи за необхідності, за погодженням з Кабінетом Міністрів України, визначають свої засвідчувальні центри, призначені для виконання функцій, зазначених у частині першій цієї статті.

Так, свій засвідчувальний центр був створений Національним банком України.

Засвідчувальний центр (ЗЦ) по відношенню до групи центрів сертифікації ключів (ГЦСК), має ті ж функції і повноваження, що й центральний засвідчувальний орган (ЦЗО) стосовно центрів сертифікації ключів (ЦСК).

Контролюючий орган (КО) - спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

Функції контролюючого органу виконує Державна служба спеціального зв’язку та захисту інформації (ДССЗЗІ).

Порядок видачі сертифікатів

Сертифікат **відкритого ключа** видається центром сертифікації ключів (ЦСК), який засвідчує чинність і належність відкритого ключа підписувачу. ЦСК завіряє сертифікат відкритого ключа своїм підписом.

Генерація особистого та відкритого ключів **для органів державної влади**, органів місцевого самоврядування, підприємств, установ та організацій державної форми власності здійснюється підписувачем в акредитованому центрі сертифікації ключів (АЦСК), що обслуговує установу, або безпосередньо в установі з використанням надійних засобів електронного цифрового підпису. З генерований особистий ключ підписувача захищається паролем та записується на носій ключової інформації.

Генерація особистого та відкритого ключів для фізичних або юридичних осіб недержавної форми власності здійснюється в центрі сертифікації ключів (ЦСК), після ідентифікації заявника та отриманих від нього даних, необхідних для формування сертифікату

З метою збереження секретності ключа, генерація особистого ключа проводиться безпосередньо самим користувачем в офісі ЦСК або АЦСК. При необхідності користувач може з генерувати ключову пару самостійно, використовуючи спеціальне програмне забезпечення. У такому випадку він повинен буде відіслати в ЦСК/АЦСК запити на формування сертифіката з відкритим ключем ЕЦП (а при необхідності - і на формування сертифіката з відкритим ключем протоколу розподілу), разом з усіма необхідними документами для реєстрації.

Особистий ключ підписувача **повинен відповідати** відкритому ключу зазначеному у сертифікаті.

Центр сертифікації ключів має право встановлювати під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу.

Центр сертифікації ключів має право надати допомогу при генерації особистих ключів. Зберігання особистих ключів підписувачів **та ознайомлення з ними** в центрі сертифікації ключів забороняються.

Підписувач зобов'язаний зберігати особистий ключ у таємниці та надавати центру сертифікації ключів дані для засвідчення чинності відкритого ключа та своєчасно надавати центру сертифікації ключів інформацію про зміну даних, відображених у сертифікаті ключа.

На виданий сертифікат встановлюється термін його дії. По закінченню цього терміну власнику видається новий сертифікат.

Видані сертифікати зберігаються в базі даних дійсних сертифікатів ЦСК і стають доступними для всіх користувачів через телекомунікаційні мережі (Інтернет).

Операції перевірки дійсності ЕЦП здійснюються автоматично, за допомогою спеціального програмного забезпечення.

При перевірці ЕЦП, сторона, що перевіряє ЕЦП звертається до бази даних дійсних сертифікатів ЦСК та отримує сертифікат відкритого ключа сторони, що перевіряється. Після перевірки статусу сертифіката, з нього витягується відкритий ключ і проводиться перевірка ЕЦП.

Фізичні особи та юридичні особи недержавної форми власності можуть, на договірних засадах, використовувати електронний цифровий підпис і **без сертифіката** ключа. У такому випадку використовуються так звані само підписані сертифікати. Особистий, відкритий ключі та сертифікати генеруються самими користувачами за допомогою спеціального програмного забезпечення, такого, наприклад, як програма с вільним розповсюдженням GNU Privacy Assistant.

Посилений сертифікат відкритого ключа - сертифікат ключа, виданий **акредитованим** центром сертифікації ключів (АЦСК), засвідчувальним центром (ЗЦ) або центральним засвідчувальним органом (ЦЗО).

У посиленому сертифікаті відкритого ключа додатково зазначаються ідентифікаційні дані установи (повне найменування та код згідно з ЄДРПОУ, за якими здійснено її державну реєстрацію).

Посилений сертифікат ключа в обов'язковому порядку повинні використовувати:

- органи державної влади;
- органи місцевого самоврядування;
- підприємства, установи та організації державної форми власності;
- державні реєстратори прав на нерухоме майно;
- державні реєстратори юридичних осіб, фізичних осіб - підприємців та громадських формувань
- нотаріуси.

У посиленому сертифікаті відкритого ключа, що використовується установою для електронної печатки, додатково зазначаються спеціальне призначення електронного цифрового підпису та сфера його застосування.

У разі необхідності один документ може бути завірений кількома ЕЦП. Перший електронний підпис, що поставлений на вихідний документ називається первинним підписом.

До документа, підписаного первинним підписом, можуть бути додані додаткові підписи інших користувачів (наприклад, при узгодженні документа співробітниками одного відділу). При цьому додаткові і первинний підписи матимуть рівний статус.

Первинний підпис може бути завірено підписом іншого користувача (наприклад, при узгодженні документа з начальником відділу). У цьому випадку буде побудовано ланцюжок (ієрархію) підписів на файлі: підпис, що завіряє і первинний підпис будуть нерівнозначними.

При наявності цифрового сертифіката електронним цифровим підписом можна підписувати документи, створені в звичайних офісних програмах, в таких, наприклад, як Microsoft Office або Adobe Photoshop.

Після припинення виконання підписувачем посадових обов’язків, для яких генерувалися особистий та відкритий ключі, підписувач або установа звертається до акредитованого центру сертифікації ключів для скасування посиленого сертифіката його відкритого ключа, а особистий ключ знищується методом, що не допускає можливості його відновлення.

Порядок застосування ЕЦП в банківській системі України та суб'єктами переказу коштів

Постановою Правління Національного банку України №78 від 14 серпня 2017 року «Про затвердження Положення про застосування електронного підпису в банківській системі України» визначені види електронного підпису, що застосовуються в банківській системі України, встановлені вимоги щодо застосування кожного з видів електронного підпису і встановлені вимоги до створення та зберігання електронних документів в банківській системі.

Встановлено, що ЕП є обов'язковим реквізитом електронного документа. Накладанням ЕП завершується створення електронного документа.

У цьому Положенні використовуються такі терміни, як:

Простий електронний підпис (ПЕП) - будь-який вид ЕП (крім ЕЦП).

Сфера застосування ПЕП:

- системи дистанційного обслуговування (тільки для фізичних осіб, шо не є суб'єктами підприємницької діяльності).

Простий електронний цифровий підпис (ПЕЦП) - ЕЦП, що застосовується сторонами на договірних засадах.

Сфера застосування ПЕЦП:

- внутрішні системи автоматизації банку;
- системи дистанційного обслуговування.

Електронний цифровий підпис Національного банку України (ЕЦП НБУ) - ЕЦП, що використовується в платіжних системах Національного банку України та інформаційних задачах Національного банку України згідно з нормативно-правовими актами Національного банку України.

Сфера застосування ЕЦП НБУ:

- система електронних платежів Національного банку;
- інформаційні задачі НБУ.

Електронний цифровий підпис, прирівняний до власноручного підпису (ЕЦП ПдВП) - ЕЦП, який за своїм статусом прирівняний до власноручного підпису відповідно до Закону України «Про електронний цифровий підпис».

Сфера застосування ЕЦП ПдВП:

- електронний документообіг;
- взаємодія з державними органами;
- оформлення електронних копій з паперових документів тощо.

Електронний цифровий підпис юридичної особи (ЕЦП ЮО) - вид ЕЦП, що забезпечує можливість перевірки цілісності електронних даних, що підписуються, та ідентифікацію юридичної особи як підписувача.

Сфера застосування ЕЦП ЮО:

- надання послуг в електронній формі;
- інформаційний обмін з іншими суб'єктами електронної взаємодії.

Завдання до лабораторної роботи

Метою виконання даної роботи є практичне ознайомлення студентів з поняттями «сертифікат відкритого ключа», «відкритий ключ», «особистий ключ», отримання навичок шифрування і роз шифровки текстових повідомлень і застосування на практиці електронного цифрового підпису.

Для обміну шифрованими повідомленнями кожна зі сторін, що бере участь в обміні, повинна мати свій сертифікат відкритого ключа. Цей сертифікат повинен бути доступним для всіх сторін, які беруть участь у такому обміні.

Для створення сертифікатів, управління та обміну ними існує спеціальне програмне забезпечення, таке, наприклад, як програма Kleopatra, що входить до складу програмного пакету Gpg4win.

Для створення шифрованого повідомлення необхідно попередньо отримати публічний сертифікат відкритого ключа іншої сторони, якій буде відправлено повідомлення і використовувати його при шифруванні повідомлення.

У свою чергу, для того, щоб створити шифрування повідомлення для вас, інша сторона повинна використовувати ваш сертифікат відкритого ключа.

Існує кілька способів обміну сертифікатами відкритого ключа:

1. пересилання сертифікату іншій стороні по електронній пошті;
2. розміщення сертифіката на сервері сертифікатів OpenPGP;
3. розміщення сертифіката на своїй веб-сторінці в Інтернет;
4. використання для передачі сертифіката якого-небудь носія (флеш-драйв («флешка»), смарт-карта і т.д.).

В ході виконання лабораторної роботи кожен студент повинен виконати наступну послідовність завдань:

1. За допомогою програми Kleopatra створити персональний сертифікат відкритого ключа. При цьому буде з генеровано відкритий і закритий ключі користувача.
2. Створити резервну копію ключів та сертифікату.
3. Надати доступ до свого сертифікату одним з описаних вище способів.
4. Отримати доступ до сертифіката іншої сторони.
5. Створити повідомлення і зашифрувати його за допомогою сертифіката ключа іншої сторони.
6. Відправити це шифрування повідомлення іншій стороні.
7. Отримати шифрування повідомлення іншої сторони і розшифрувати його за допомогою отриманого раніше сертифіката відкритого ключа.

Апаратне і програмне забезпечення для виконання завдання:

1. Персональний комп'ютер з операційною системою Windows, підключений до мережі Інтернет.
2. Встановлений на комп'ютері програмний пакет Gpg4win (програма с вільним розповсюдженням), що включає в себе програми Kleopatra і GNU Privacy Assistant.

Завдання 1

Створення персонального сертифіката відкритого ключа:

1. Запустити на комп'ютері програму Kleopatra (входить до складу пакету Gpg4win).
2. У вікні Kleopatra вибрати меню File, потім пункт New Certificate (рис 1.).

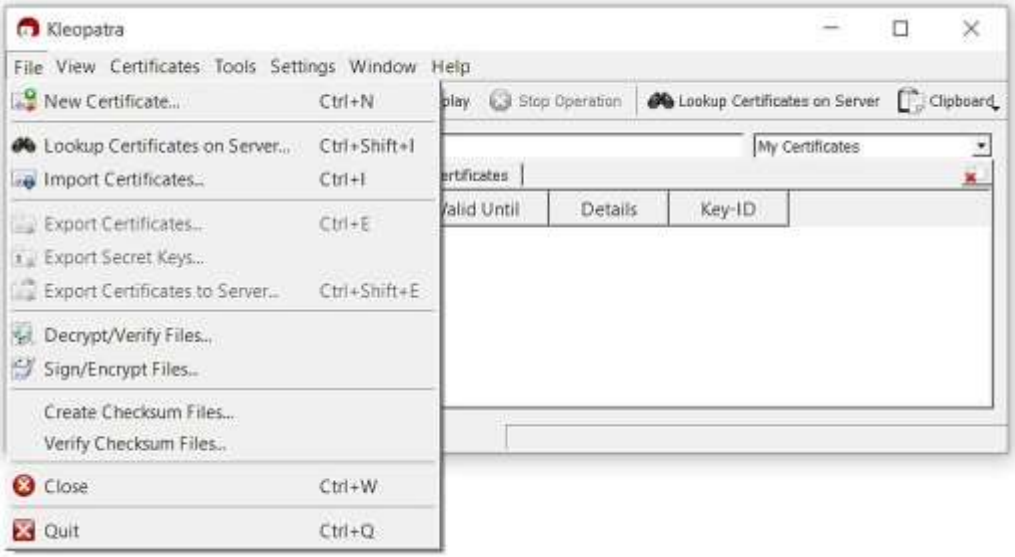


Рис. 1

3. У вікні «Choose Certificate Format» вибрати пункт «Create a personal OpenPGP key pair», і натиснути кнопку Next (рис 2.).

Рис. 2

4. У вікні «Enter Details» ввести своє прізвище і ім'я (латинськими буквами), ввести отриманий раніше адрес своєї електронної пошти і натиснути кнопку Next (рис 3.) У наступному вікні натиснути кнопку «Create Key».

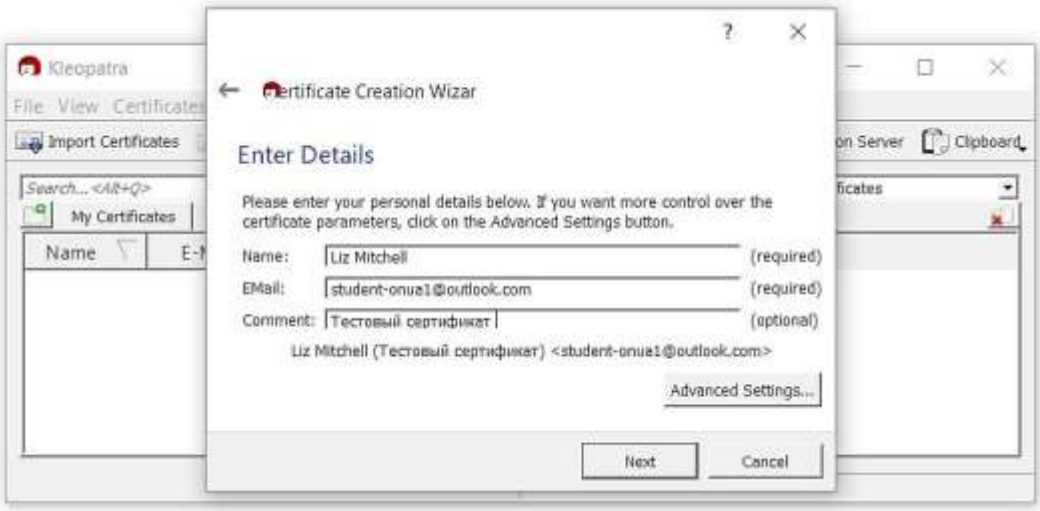


Рис. 3

5. У вікні «pinentry» ввести пароль. Пароль повинен складатися з восьми символів, частина з яких повинна бути цифрами (наприклад: odessa2017). Підтвердіть введення пароля. Запишіть пароль.
6. Після повторного введення пароля почнеться процес генерації ключової пари і створення сертифіката. На повільних комп'ютерах процес генерації ключів може тривати досить довго.
7. Після завершення генерації у вікні Kleopatra повинен з'явитися відповідний напис з ім'ям сертифіката (ім'я сертифіката включає прізвище користувача і його адресу електронної пошти). В результаті виконання даної операції була створена пара ключів (відкритий та особистий ключі) і сертифікат відкритого ключа.

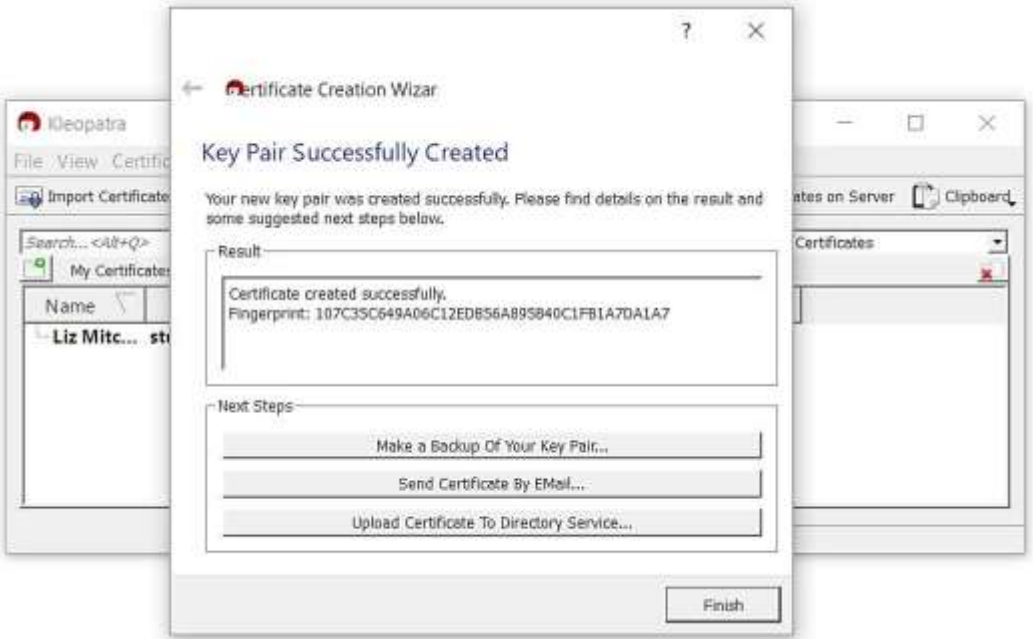


Рис. 4

8. Зберегти резервну копію сертифіката закритого ключа в своїй папці, наприклад, в папці KeyBackup. Для цього на диску D слід створити папку «KeyBackup», потім в вікні «Key Pair Successfully Created» потрібно натиснути кнопку «Make a Backup Of Your Key Pair...».
9. У вікні «Export Secret Certificate» (рис. 5) встановити прапорець «ASCII armor», вказати в рядку «Output file:» шлях D:\KeyBackup, ввести ім'я сертифіката з розширенням «.asc» і натиснути кнопку ОК. Переконатися в тому, що резервна копія сертифіката була створена.

Рис. 5

10. Знайти на комп'ютері за вказаним шляхом файл секретного ключа з розширенням ***.asc** і відкрити цей файл за допомогою програми Блокнот.
11. Знайти в текстовому файлі блок, що містить код закритого (PGP PRIVATE KEY BLOCK) ключа.
12. Провести експорт сертифіката відкритого ключа. Для цього у вікні Kleopatra необхідно натиснути на кнопку «Export Certificates» та вказати шлях до папки KeyBackup на диску D.
13. Знайти на комп'ютері за вказаним шляхом файл сертифіката відкритого ключа з розширенням ***.asc** і відкрити цей файл за допомогою програми Блокнот.
14. Знайти в текстовому файлі блок, що містить код відкритого (PGP PUBLIC KEY BLOCK) ключа.
15. Будь-який загальний доступ до файлу, який містить закритий ключ не допускається. Цей файл повинен бути збережений в надійному місці, недоступному для сторонніх осіб.

Завдання 2

Надання доступу до сертифіката відкритого ключа:

1. Сертифікат відкритого ключа можна надіслати електронною поштою як у вигляді тексту, так і у вигляді вкладеного файлу. У першому випадку слід скопіювати вміст файлу сертифіката відкритого ключа у вікно створення поштового повідомлення. При цьому слід пам'ятати, що в налаштуваннях поштової програми повинна бути встановлена настройка «Відправляти повідомлення в текстовому вигляді» (а не в форматі HTML).
2. Сертифікат відкритого ключа можна передати у вигляді файлу на будь-якому комп'ютерному носії (наприклад, за допомогою USB флеш-накопичувача).
3. Найбільш зручним для всіх способом передачі є розміщення сертифіката відкритого ключа на сервері сертифікатів OpenPGP.
   Для цього необхідно у вікні Kleopatra вибрати меню File, потім пункт «Export Certificates to Server» (рис. 6). Підтвердити відправку сертифіката.

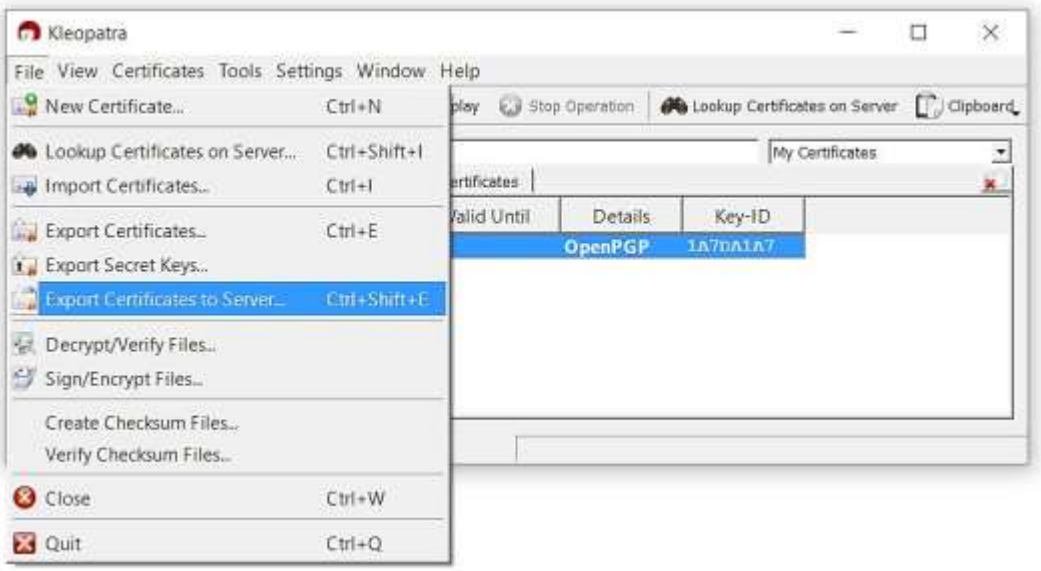


Рис. 6

4. Після відправки сертифіката на сервер він стане доступним для всіх бажаючих.

Завдання 3
Імпорт сертифіката відкритого ключа:

1. Для перегляду розміщеного на сервері сертифіката необхідно скористатися кнопкою «Lookup Certificates on Server».
   Для пошуку сертифіката в базі даних сертифікатів, необхідно ввести його ім'я (або адресу електронної пошти) (рис. 7).

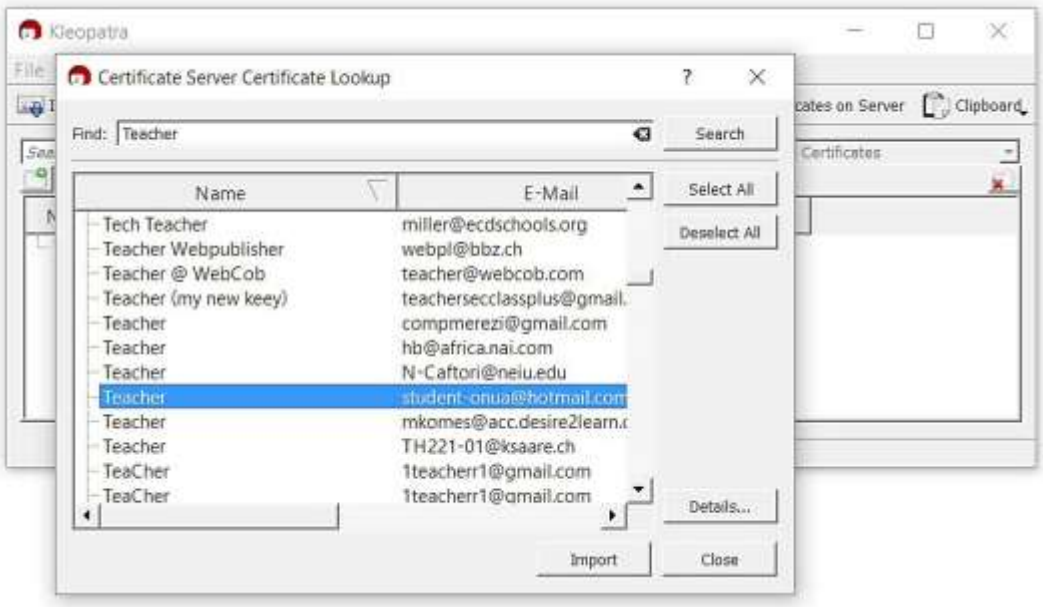


Рис. 7

2. Для виконання даного завдання необхідно в поле «Find:» ввести ім'я сертифіката «Teacher», натиснути кнопку Search і у вікні результатів пошуку

знайти сертифікат Teacher з адресою електронної пошти student-onua@hotmail.com.

Знайдений сертифікат необхідно імпортувати в програму, натиснувши кнопку «Import».

3. Якщо сертифікат відкритого ключа був отриманий у вигляді файлу, то для його імпорту досить натиснути кнопку «Import Certificates» у вікні Kleopatra та вказати шлях до файлу сертифіката.

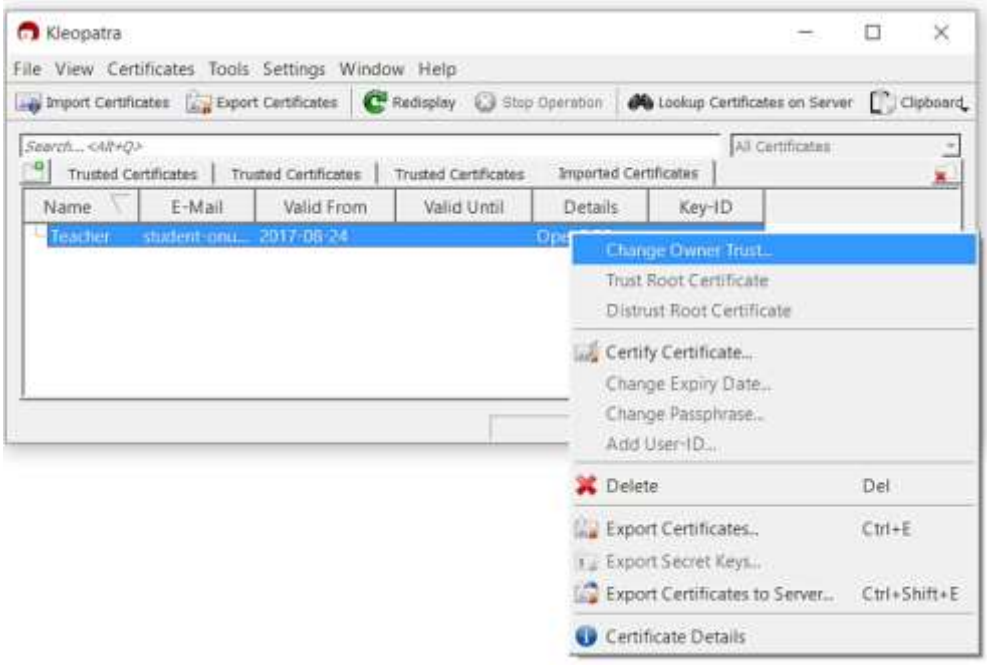


Рис. 8

4. Для встановлення ступеня довіри до сертифіката необхідно викликати контекстне меню та вибрати пункт «Change Owner Trust» (рис. 8).

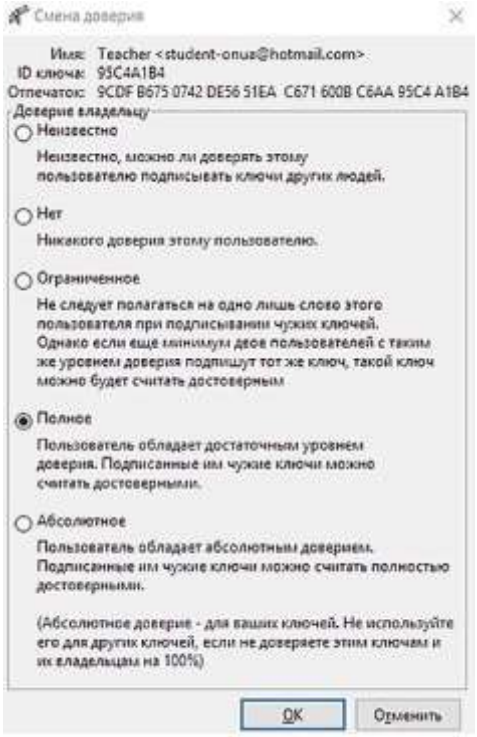


Рис. 9

5. У вікні «Зміна довіри» можна вибрати один з п'яти варіантів рівня довіри користувачеві даного сертифікату відкритого ключа (рис. 9).
6. Встановіть рівень довіри «Повний» (I believe checks are very accurate).

Завдання 4

Проведення сертифікації без використання ЦСК або АЦСК:

1. Достовірність зашифрованого повідомлення може бути підтверджена його відправником за допомогою ЕЦП. Для того, щоб програма змогла перевірити ЕЦП відправника, сертифікат цієї ЕЦП повинен бути попередньо кимось сертифікований. Зазвичай таку сертифікацію проводять ЦСК або АЦСК. Але якщо вимоги до надійності сертифіката не настільки суворі, то сертифікацію можна проводити і звичайним користувачам. Довіра до таких сертифікатів буде обмеженою.
2. Для проведення сертифікації самим користувачем у вікні Kleopatra необхідно вибрати сертифікат, для якого необхідно провести процедуру сертифікації. Потім слід натиснути правою кнопкою миші по вибраному сертифікату і вибрати пункт «Certify Certificate» (рис. 10).

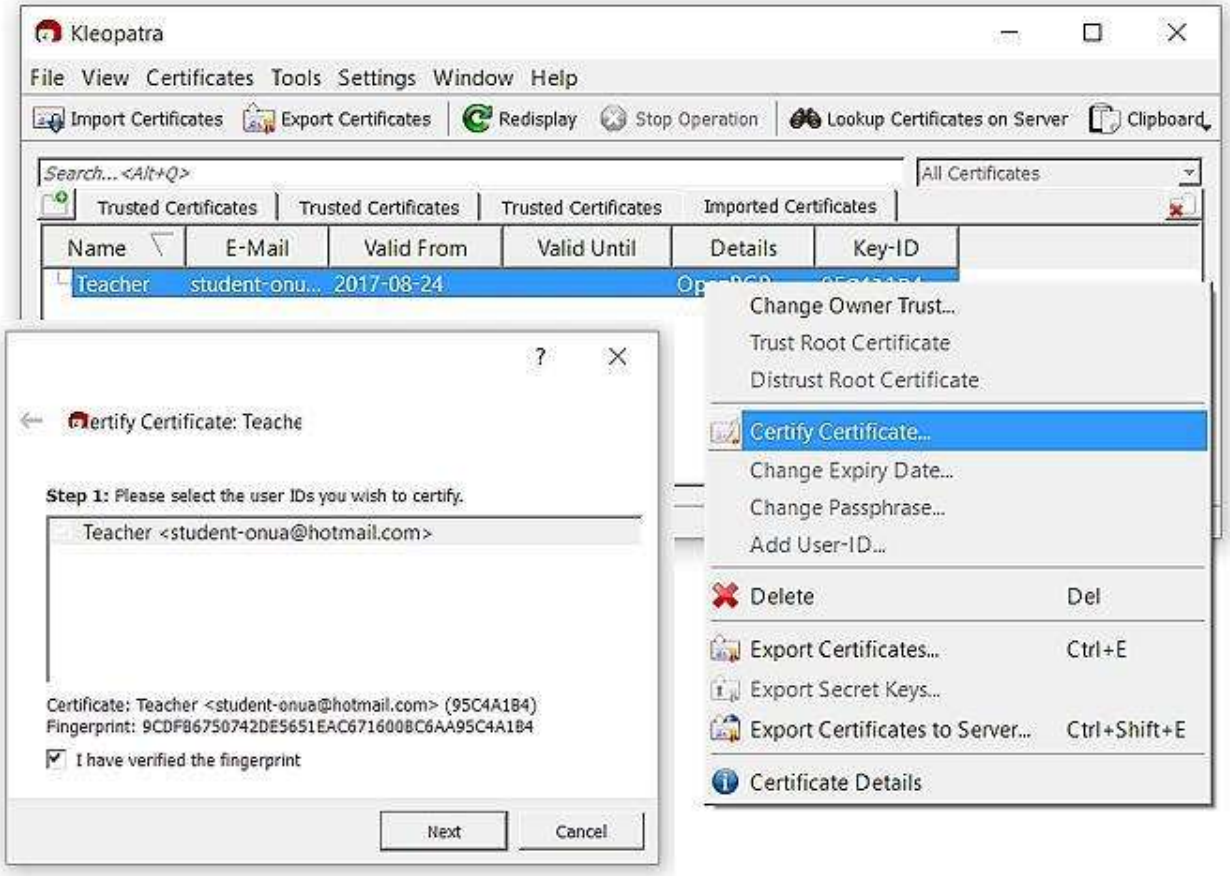


Рис. 10

3. У вікні «Certify Certificate: Teacher» (рис. 10) необхідно встановити прапорці в пунктах «Teacher <student-onua@hotmail.com>» і «I have verified the fingerprint» та натиснути кнопку Next.
4. У наступному вікні необхідно встановити прапорець в пункті «Certify only for myself» («Сертифікувати тільки для себе») і натиснути клавішу «Certify». Для підтвердження сертифікації необхідно ввести пароль (див. Пункт 5 завдання 1) та натиснути кнопку «Finish».

Завдання 5

Створення шифрованого повідомлення:

1. Знайти в Інтернет за допомогою браузера і пошукової системи текст статті у Вікіпедії «Асиметричне шифрування» і скопіювати частину цього тексту.

2. Відкрити програму Блокнот, ввести в перший рядок своє ім'я, прізвище і номер групи.
3. У другому рядку - вставити скопійований раніше текст.
4. Зберегти текстовий документ з іменем «**LR-1**» на Робочому столі.
5. У вікні Kleopatra вибрати меню File, потім пункт меню «Sign/Encrypt Files». Вибрати на Робочому столі файл «LR-1».

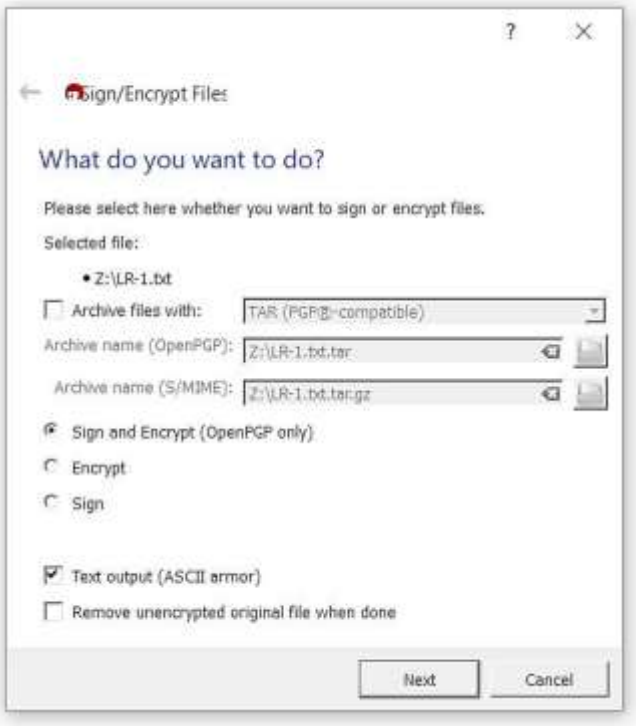


Рис. 11

6. Для накладення на зашифроване повідомлення електронного цифрового підпису - у вікні «Sign/Encrypt File» необхідно встановити прапорець «Sign and Encrypt (OpenPGP only)».
7. У вікні «Sign/Encrypt File» необхідно встановити прапорець «Text output (ASCII armor)» і натиснути кнопку «Next» (рис. 11).

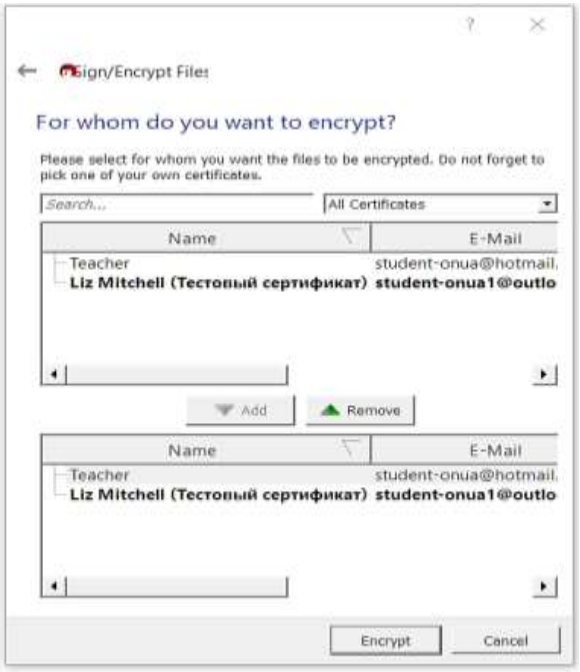


Рис. 12

1. У вікні «For whom do you want to encrypt?» слід вибрати сертифікат відкритого ключа одержувача шифрованого повідомлення (в даному випадку - сертифікат «Teacher»). Цей відкритий ключ буде використаний для шифрування повідомлення.
2. Потім слід вибрати свій власний сертифікат закритого ключа, за допомогою якого на шифрування повідомлення буде накладений ЕЦП відправника (в даному випадку (рис. 12) - це сертифікат «Liz Mitchell»).
3. Після натискання на кнопку «Encrypt» буде вироблено шифрування файлу. По закінченню шифрування з'явиться вікно з результатами шифрування, в якому необхідно натиснути на кнопку «Finish».
4. Відкрити Робочий стіл і переконатися в тому, що в цій папці з'явився файл з іменем **LR-1.txt.asc**, що містить шифрування повідомлення. За допомогою програми Блокнот відкрити цей файл і знайти текстовий блок, що містить шифрування повідомлення (PGP MESSAGE). Закрити цей файл без збереження змін.
5. Передати файл **LR-1.txt.asc** викладачеві (по електронній пошті або за допомогою флеш-накопичувача) для контролю виконання роботи.

Практична робота

Тема Застосування криптографічних засобів захисту інформації. Формування пар відкритих та закритих ключів для реалізації асиметричного шифрування.

МЕТА: Формування вмінь і навиків організації криптографічного захисту інформації. Отримання знань методів і способів асиметричного шифрування та навиків використання відповідного програмного забезпечення. Закріплення знань файлової структури, вмінь і навиків використання можливостей диспетчерів файлів та поштових систем для пересилання файлів іншим користувачам.

- Головне вікно Cyber Safe містить:

Основне меню. Надає доступ до основних функцій програми. Пункти меню містять додаткові випадаючі вкладки, що відповідають вибраній категорії.

Меню опцій. Містить опції створення, експорту, імпорту, публікації, пошуку і видалення, всі або деякі з яких можуть бути застосовані до файлів, папок, дисків та сертифікатів.

Ключі та сертифікати. Доступні вкладки "Усі ключі", "Мій закритий ключ", а також функція "Пошук ключів" (в результаті пошуку видаються дані, які ґрунтуються на імені або електронну адресу користувачів).

Шифрування файлів. Доступ до функцій щодо шифрування і дешифрування файлів, створення та перевірки цифрового підпису.

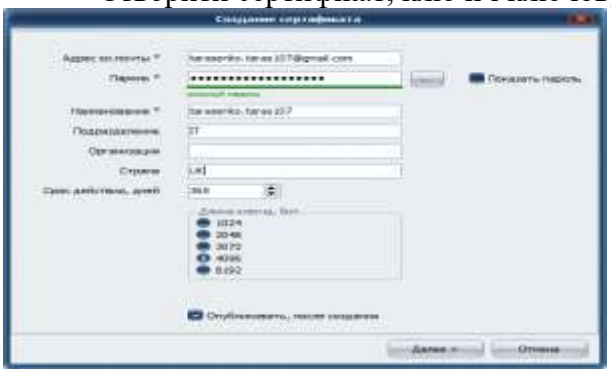
Шифрування дисків. Доступ до функцій щодо шифрування логічних дисків і їх розділів, створення віртуальних зашифрованих дисків, а також зберігання ключів на токенах.

Робоча область Cyber Safe. Відображає інформацію, а також дії, які можуть бути зроблені відповідно до вибраного пунктом меню.

Всі блоки вертикального меню під номерами 3, 4, 5 спочатку відображаються в розгорнутому вигляді. Пункти Меню опцій, а також зміст Робочої області змінюється в залежності від того, який з пунктів в меню вибрано. Наприклад, при виборі функції **Шифрування файлів** в

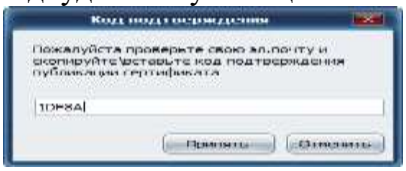
Робочій області відобразиться можливість вибору одного з двох варіантів шифрування (для особистого користування або пересилання іншим користувачам), а в Меню опцій будуть доступні опції: додати папку, додати файл, видалити та показати. А при виборі пункту меню **Всі ключі** в Робочій області з'явиться список всіх доступних ключів на вашій зв'язці, та в Меню опцій відобразяться опції: створити, експорт, публікація, імпорт, пошук і видалити.

- Запустити програму CyberSafe
- Створити сертифікат, ключі і ключову пару, як показано на мал



Створення ключової пари в CyberSafe відбувається при створенні сертифіката, створені ключі зберігаються в базі даних програми і, при необхідності, можуть бути експортовані в окремі файли.

В полі Email Address вказуємо свій діючий електронний адрес, на який буде висланий код що необхідний для публікації сертифіката на сервері. Пропонується заповнити і необов'язкові поля, які будуть відображені у вашому сертифікаті. Вибираємо розмір ключа шифрування в межах від 1024 до 4096 біт, а також термін його дії. Після процесу генерації ключа сертифіката на вказаний вами e-mail буде висланий код, який потрібно ввести у відповідне поле, після чого відбудеться публікація вашого сертифіката на сервері.



Після успішного підтвердження процедура по створенню сертифіката завершена. Результат можна побачити в головному вікні програми.

- Щоб переглянути ключі на локальній зв'язці, відкрийте CyberSafe і в пункті меню **Ключі та Сертифікати** (Keys and Certificates) виберіть:
- **Всі ключі** (All Keys). Це показує всі ключі на вашій зв'язці.
- **Особисті ключі** (Private Keys). Це показує лише закриті ключі на вашій зв'язці.
- **Пошук ключа** (Search for Keys). Пошук ключа на вашій зв'язці виходячи із зазначених критеріїв.

Ваші **Особисті ключі** мають значок  і містять ваш відкритий і закритий ключі. Ключі інших користувачів, які відображаються на зв'язці **Всі ключі** разом з вашими особистими ключами, мають значок  і містять тільки відкриті ключі цих користувачів.

- Створити резервну копії ключів

В меню Ключі та Сертифікати виберіть пункт **Особисті ключі.**

В робочій області в списку ключів виділіть потрібний ключ і натисніть **Експорт**. У діалоговому вікні введення пароля введіть свій пароль для даного ключа (сертифіката).

У діалоговому вікні програми виберіть **Експорт ID файлу** і вкажіть місце на локальному комп’ютері або змінному носії, куди будуть експортовані ключі. натисніть Прийняти:

Експортований файл, який містить ваш закритий і відкритий ключі, має розширення * .id. Пам’ятайте, що цим файлом не потрібно ділитися з іншими користувачами, так як він містить ваш закритий ключ.

УВАГА!!! Якщо ваш закритий ключ загублений і у вас немає його резервної копії, ви більше ніколи не зможете розшифрувати інформацію, зашифровану вами або іншими користувачами за допомогою відкритих ключів. Така інформація буде корисною і не підлягає відновленню.

- Самостійно проведіть публікацію відкритого ключа на сервері вручну

ПРИМІТКА Як тільки ваш відкритий ключ розміщений на сервері, він стає доступним для користувачів, які хочуть відправити вам зашифровані дані або перевірити ваш цифровий підпис. Навіть, якщо ви безпосередньо не покажете користувачам ваш відкритий ключ, вони можуть отримати його копію за допомогою функції пошуку на сервері ключів, використавши для цього ваше ім'я або адресу електронної пошти.

Багато користувачів включають web-адресу свого відкритого ключа в кінці своїх e-mail повідомлень. У більшості випадків, одержувачу такого e-mail досить просто кликнути на адресу для того, щоб отримати копію відкритого ключа на сервері. Деякі навіть розміщують унікальні електронні відбитки своїх відкритих ключів на своїх візитних картках для спрощення їх перевірки.

- Самостійно проведіть шифрування і дешифрування файлів на основі сертифікатів (ключів). Аналогічно опрацюйте шифрування файлів паролем.
- Самостійно проробіть прозоре шифрування на локальному комп’ютері

Самостійно опрацювати питання:

Описати пункти в звіті:

Переміщення CyberSafe з одного комп’ютера на інший.

Заходи, що використовуються для захисту ключів

Використання флеш-накопичувача в якості токена