ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖЕНИЙ
ЄААД.00021-13-ЛЗ

АТ ІІТ
Користувач ЦСК
Програмний комплекс користувача ЦСК

ІІТ

Інв. № орига.	
Підп. та дата	
Взам. інв. №	
Інв. № дубл	
Підп. та дата	

Програмний комплекс користувача ЦСК (ОС Google Android)

Версія 1.3.1

Настанова оператора

ЄААД.00021-13 34 30-2

Харків 2015 р.

АНОТАЦІЯ

Даний документ містить настанову оператора для роботи з програмним комплексом користувача центра сертифікації ключів (далі - програма). Настанова містить відомості щодо порядку використання програми.

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

ЗМІСТ

1 ПРИЗНАЧЕННЯ ПРОГРАМИ

Програма призначена для застосування на засобах ЕОТ користувача центра сертифікації ключів і виконує наступні функції:

- управління ключами користувача:
  - генерацію ключів користувача ЦСК, запис особистого ключа на НКІ та формування запита на формування сертифіката;
  - перевірку сформованого сертифіката користувача на відповідність запиту;
  - формування запита на формування нового сертифіката;
- доступ до сертифікатів ЦСК, серверів ЦСК, сертифікатів інших користувачів та СВС:
  - пошук сертифікатів у файловому сховищі, LDAP-каталозі та за допомогою протоколу OCSP;
  - визначення статусу сертифікатів за допомогою СВС та за протоколом OCSP;
  - перевірку чинності та цілісності сертифікатів та ін.;
- захист файлів користувача:
  - підпис файлів;
  - перевірку файлів;
  - зашифрування файлів;
  - розшифрування файлів.

2 УМОВИ ВИКОНАННЯ ПРОГРАМИ

Програма може бути завантажена та виконана на пристроях під керуванням ОС Android 2.3.5 або вище.

Примітка. Відомості щодо послідовності та особливостей інсталяції програми, а також встановлення параметрів роботи наведені в настанові системного програміста (ЄААД.00021-13 32 30-2).

3 УПРАВЛІННЯ СЕРТИФІКАТАМИ ТА СВС

3.1 Перегляд сертифікатів

Після запуску на екрані буде відображене головне вікно програми, що наведене на рис. 3.1. Мова інтерфейсу залежить від поточної мови системи. Програма підтримує три мови інтерфейсу: українську, російську та англійську.

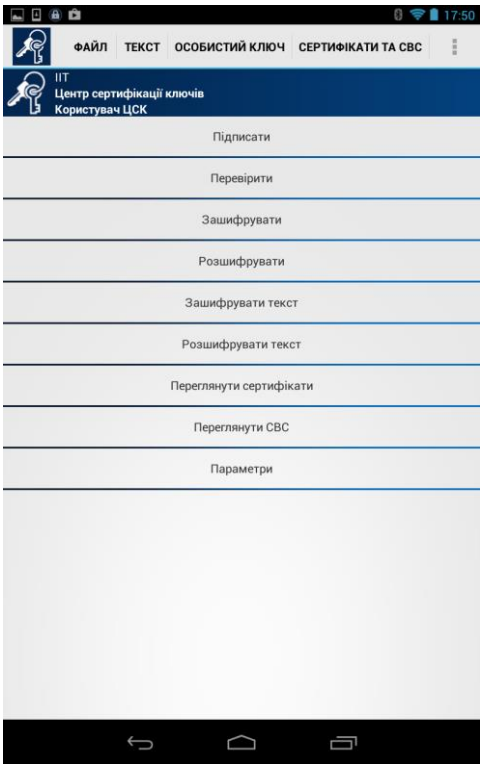

Рисунок 3.1

Для перегляду сертифікатів що містяться у файловому сховищі необхідно обрати пункт меню “Переглянути сертифікати” (рис. 3.1). Вікно із сертифікатами наведене на рис. 3.2.

За допомогою даного вікна можна переглядати сертифікати.

Сертифікати у вікні відсортовані за типами власників (тип власника обирається у верхній частині вікна):

- сертифікати користувачів ЦСК;.
- сертифікати серверів ЦСК;
- сертифікати ЦСК.

Для перегляду списку сертифікатів власника певного типу необхідно обрати відповідний тип власника у верхній частині вікна.

Для перегляду сертифіката необхідно натиснути на відповідному записі про сертифікат у списку. Сертифікат буде відображено у вікні що наведене на рисунках 3.3.

Рисунок 3.2

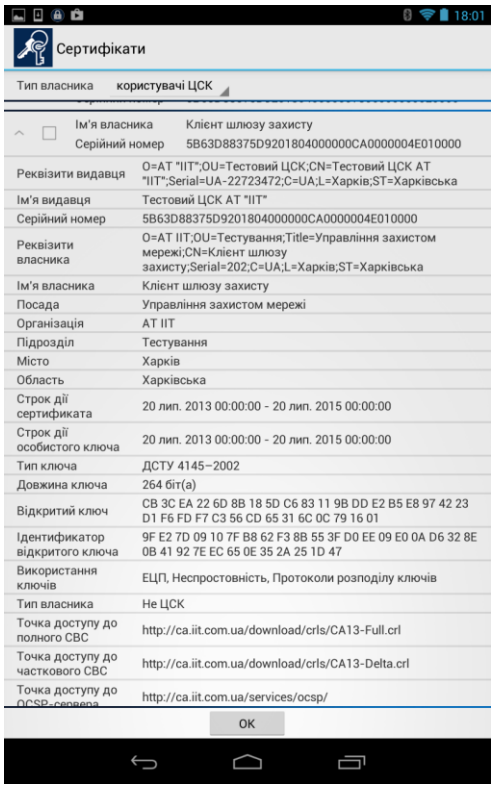

Рисунок 3.3

3.2 Перегляд СВС

Для перегляду списків відкликаних сертифікатів (СВС) необхідно обрати пункт меню “Переглянути СВС” (рис. 3.1). Вікно із списками відкликаних сертифікатів наведене на рис. 3.4.

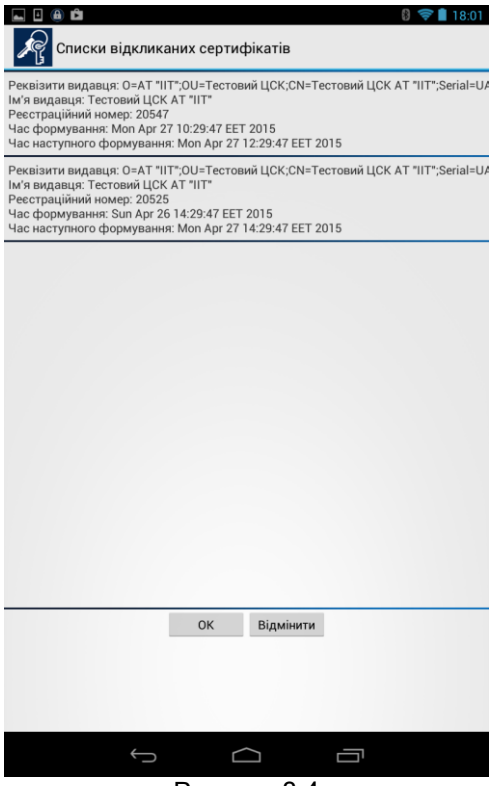

Рисунок 3.4

Для перегляду СВС необхідно натиснути на відповідному записі про СВС у списку. СВС буде відображено у вікні що наведене на рисунках 3.5.

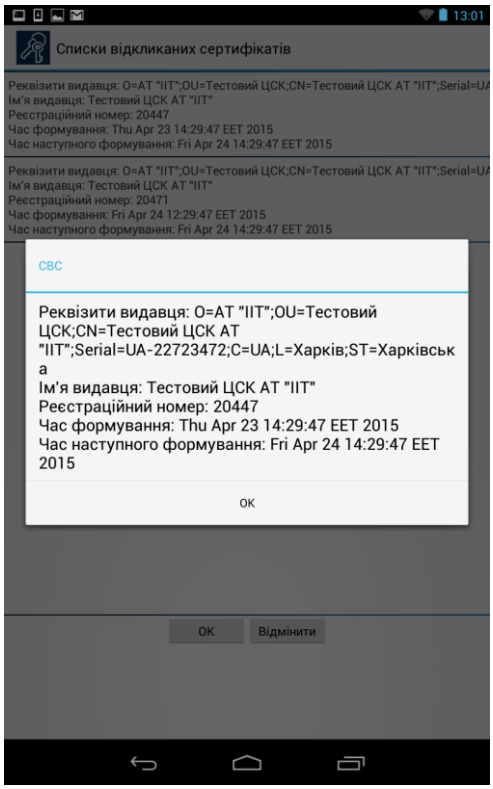

Рисунок 3.5

Пор. № зміни	Підпис відпов. особи	Дата внесення

4 УПРАВЛІННЯ КЛЮЧАМИ

4.1 Генерація ключів

Для генерації ключів необхідно обрати підпункт “Згенерувати ключі” в пункті меню “Особистий ключ” (рис. 4.1).

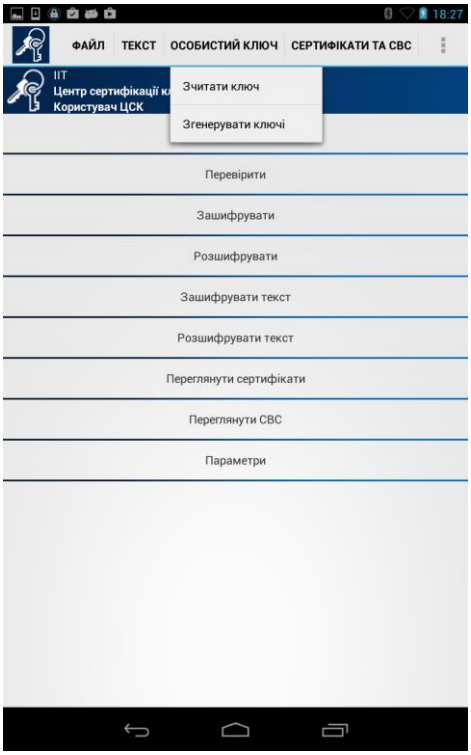

Рисунок 4.1

Вікно з першою сторінкою майстра генерації ключів наведене на рис. 4.2.

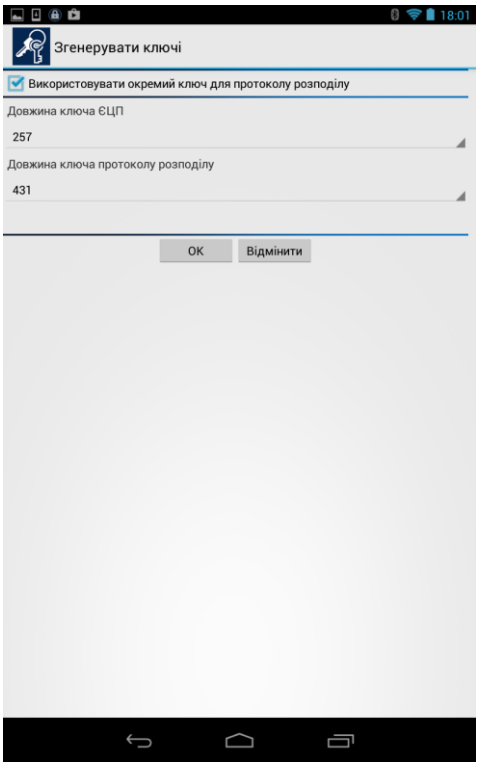

Рисунок 4.2

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

На цій сторінці обираються параметри криптографічних алгоритмів та протоколів (для більшості випадків ці параметри можна залишити за замовчанням).

Якщо параметр "Використовувати окремий ключ для протоколу розподілу" встановлено, то буде згенеровано 2 ключа: один для ЕЦП, другий для протоколу розподілу, обидва ключа зберігаються разом у файлі, та 2 запити на сертифікати: перший для сертифіката ЕЦП, другий з суфіксом KEP – для сертифіката ключа протоколу розподілу. Якщо параметр не встановлено, то буде згенеровано один ключ, що буде використовуватись як для ЕЦП, так і для за шифрування, аналогічно для запитів на сертифікати.

Генерація ключів та формування запитів на сертифікати виконується на карту пам'яті пристрою користувача. Файл ключа має назву: key-6.dat, та розташовується у кореневому каталозі карти пам'яті пристрою, зазвичай це /sdcard або /mnt/sdcard, але назва каталогу може відрізнятися в залежності від пристрою. Якщо ключі вже існують буде відображено попередження про їх перезапис (рис. 4.3). На наступній сторінці майстра (рис. 4.4) треба вказати пароль захисту особистого ключа. Запити на сертифікати зберігаються у каталозі, обраному для файлового сховища, зазвичай це каталог My Certificates and CRLs, та розташовується у кореневому каталозі карти пам'яті пристрою, Файли запиту мають назву: EU-XX-XX-XX.p10 та EU-XX-XX-XX-KEP.p10, де XX-XX-XX – це дата формування запиту у форматі День-Місяц-Рік.

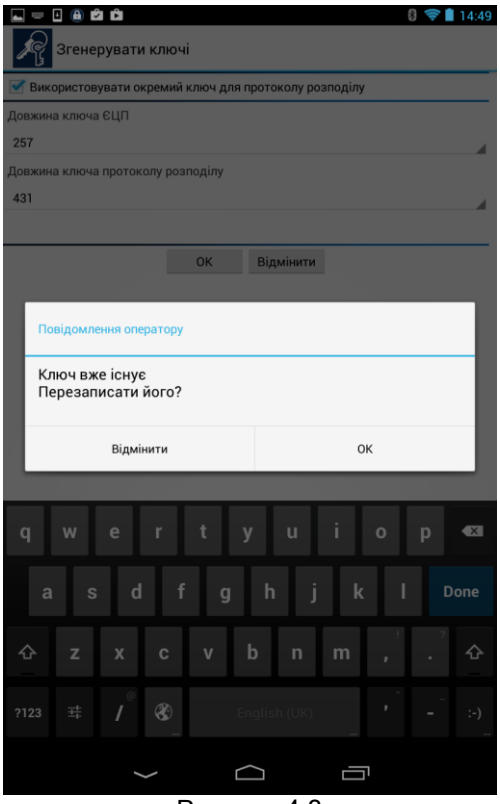

Рисунок 4.3

Пор. № зміни	Підпис відпов. особи	Дата внесення

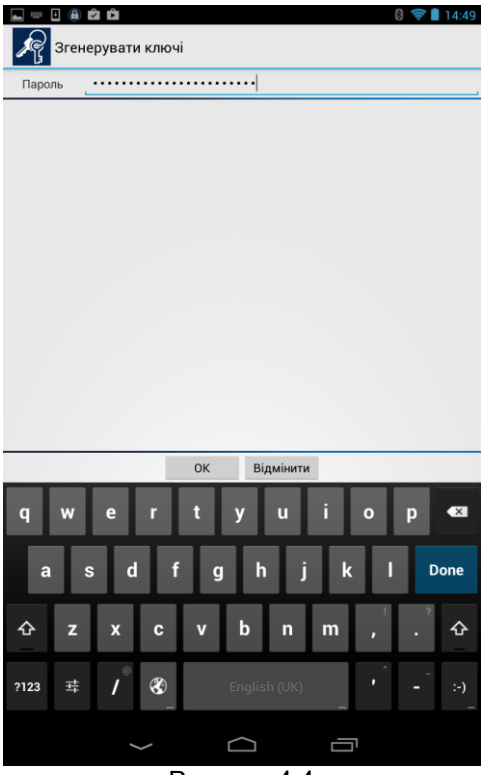

Рисунок 4.4

Пароль захисту особистого ключа повинен відповідати наступним вимогам:

- довжина - не менше 8 символів;
- не повинен містити однакові символи;
- не повинен містити підряд більше ніж 2 символи з розкладинки клавіатури;
- дозволені символи - 'a-z', 'A-Z', '0-9', '+', '-'.

Примітка. Такі вимоги носять рекомендаційний характер.

4.2 Зчитування особистого ключа

Для роботи з більшістю функцій програми (захисту файлів та ін.) необхідне попереднє зчитування особистого ключа користувача. Ініціювання зчитування особистого ключа може бути виконане автоматично при виборі певної функції програми чи виконане шляхом вибору підпункту “Зчитати ключ” в пункті меню “Особистий ключ” (рис. 4.1).

У вікні, що з’явиться (рис. 4.5) необхідно обрати тип НКІ з особистим ключем.

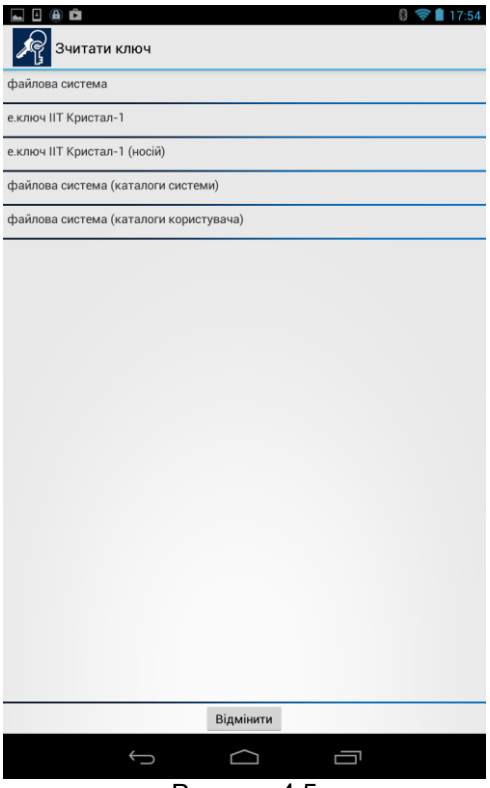

Рисунок 4.5

У вікні, що з’явиться (рис. 4.6) необхідно обрати назву носія.

Рисунок 4.6

У вікні, що з’явиться (рис. 4.7) необхідно обрати пароль захисту особистого ключа.

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

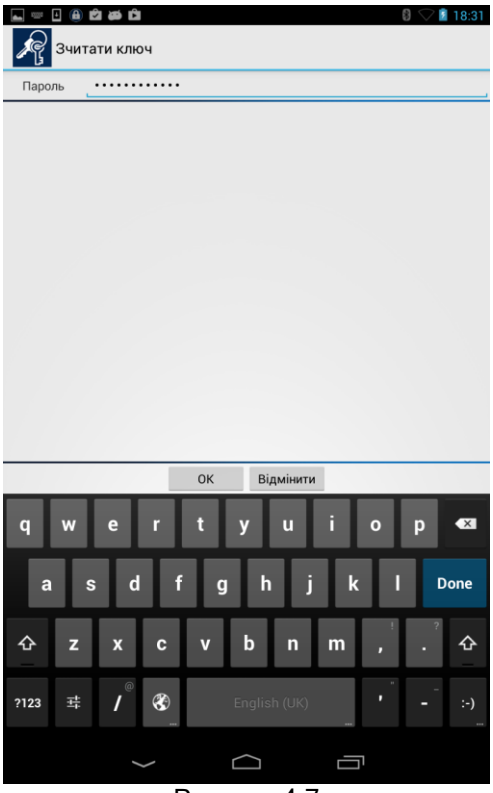

Рисунок 4.7

Інформація про те, що особистий ключ зчитаний або під час зчитування виникла помилка відображається у короткочасному попередженні.

5 ЗАХИСТ ФАЙЛІВ

5.1 Підпис файлів

Для підпису файлів (накладання ЕЦП) необхідно обрати пункт меню “Підписати” (рис. 3.1). Якщо особистий ключ ще не було зчитано, відбувається його зчитування відповідно до п. 4.2.

Вікно підпису файлів наведене на рис. 5.1. Вікно містить список файлів, які можуть бути підписні.

Файли обираються для накладання підпису за допомогою торкання екрану пристрою напроти необхідного файлу. Для скасування накладання підпису необхідно повторно торкнутися екрану пристрою напроти необхідного файлу. Кнопка з зображенням синьої стрілки використовується для пересування до каталогу на рівень вище.

Підпис додається до вихідного файлу та до розширення файлу додається суфікс “.p7s”.

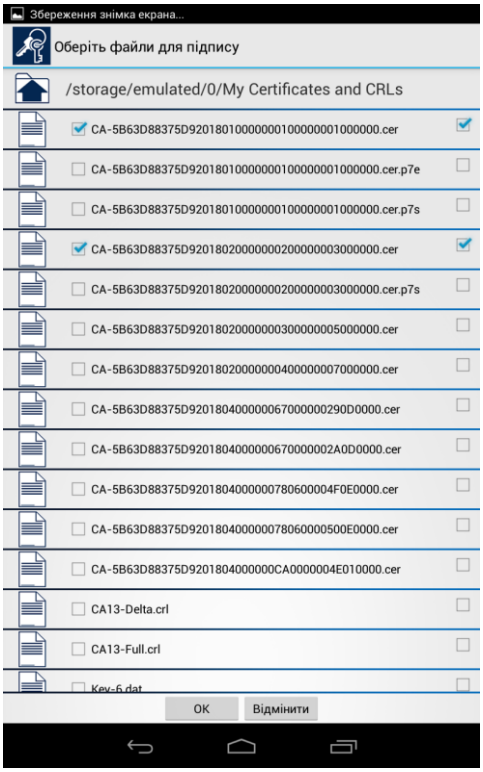

Рисунок 5.1

Для підпису файлів необхідно натиснути кнопку “OK”.

Після здійснення підпису файлів вікно буде містити інформацію про результати підпису (рис. 5.2).

Рисунок 5.2

5.2 Перевірка файлів

Для перевірки підпису (ЕЦП) необхідно обрати пункт меню “Перевірити” (рис. 3.1). Якщо особистий ключ ще не було зчитано, відбувається його зчитування відповідно до п. 4.2.

Вікно перевірки файлів наведене на рис. 5.3. Вікно містить список файлів. Файли, які можуть бути перевірені мають розширення “.p7s”. Кнопка з зображенням синьої стрілки використовується для пересування до каталогу на рівень вище.

Файли обираються для перевірки підпису за допомогою торкання екрану пристрою напроти необхідного файлу. Для скасування перевірки підпису окремого файлу необхідно повторно торкнутися екрану пристрою напроти нього.

Рисунок 5.3

Для перевірки файлів необхідно натиснути кнопку “OK”.

Після здійснення перевірки файлів вікно буде містити інформацію про результати підпису (рис. 5.4).

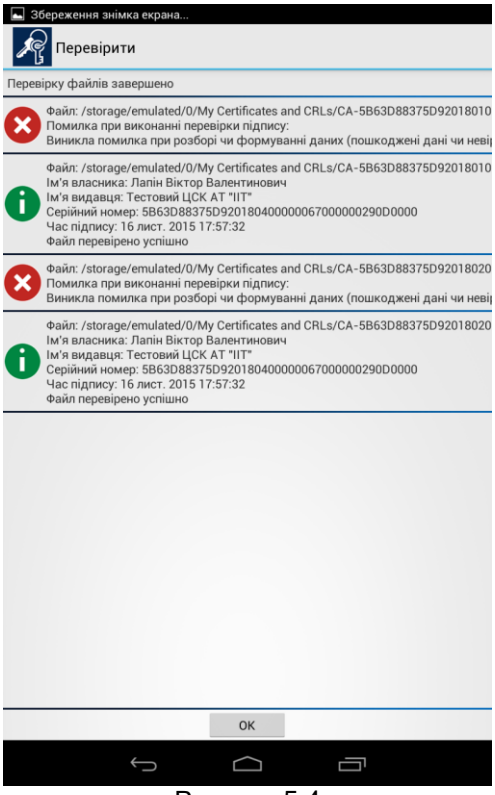

Рисунок 5.4

В разі вдалої перевірки можна також переглянути інформацію про сертифікат користувача, що підписав файл (для цього необхідно натиснути на відповідний запис про файл). Вікно наведене на рис. 5.5.

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

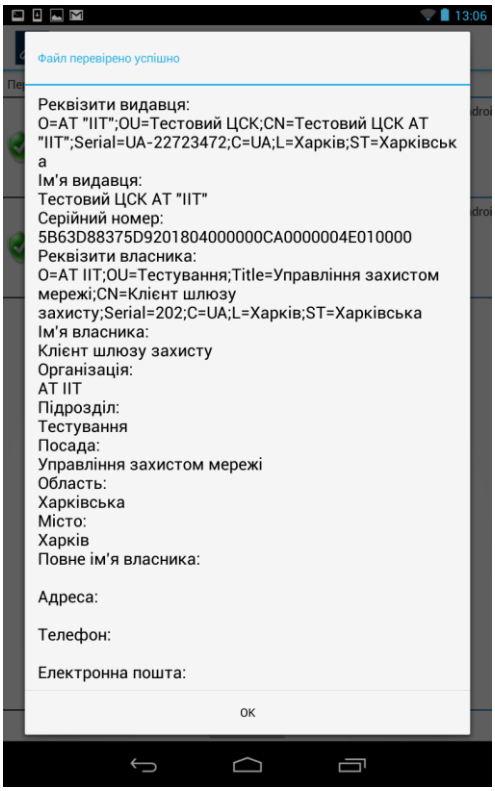

Рисунок 5.5

У детальній інформації наводяться реквізити сертифіката користувача що підписав файл.

При перевірці підпису буде створено копію файлу без підпису без розширення “.p7s”. Файл буде записаний до того ж каталогу у якому знаходився підписаний файл.

5.3 Зашифрування файлів

Для зашифрування файлу необхідно обрати пункт меню “Зашифрувати” (рис. 3.1). Якщо особистий ключ ще не було зчитано, відбувається його зчитування відповідно до п. 4.2.

Вікно зашифрування файлів наведене на рис. 5.6. Вікно містить список файлів, які можуть бути зашифровані. Кнопка з зображенням синьої стрілки використовується для пересування до каталогу на рівень вище.

Файли для зашифрування обираються за допомогою торкання екрану пристрою напроти необхідного файлу. Для скасування зашифрування необхідно повторно торкнутися екрану пристрою напроти необхідного файлу.

Вихідні зашифровані файли мають розширення “.p7e”.

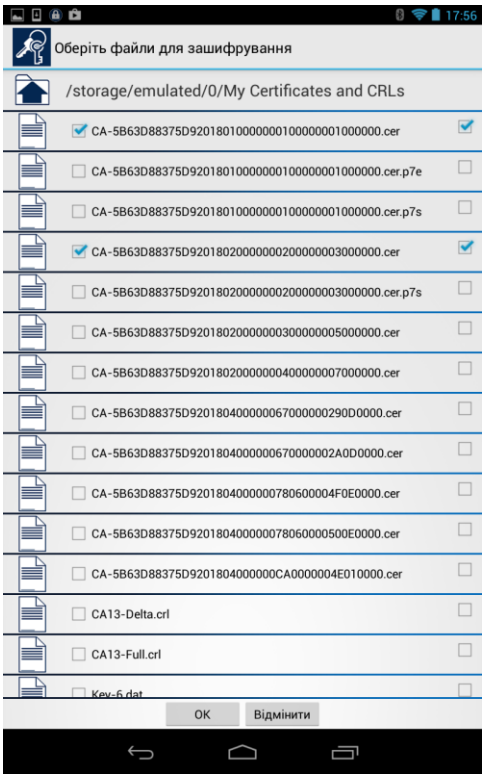

Рисунок 5.6

Для зашифрування файлів використовується особистий ключ користувача що виконує зашифрування та сертифікат(и) користувача(ів) для якого(их) зашифровується файл. Тому у вікні що наведене на рис. 5.7 необхідно обрати сертифікати користувачів для яких виконується зашифрування файлу. Зашифрований файл може бути відкритим лише користувачем для якого виконувалось зашифрування.

Рисунок 5.7

Пор. № зміни	Підпис відпов. особи	Дата внесення

Для виконання зашифрування необхідно натиснути кнопку “Зашифрувати”.

Під час шифрування здійснюється перевірка параметрів ключових даних користувачів що були обрані у списку (рис 5.7). Якщо параметри ключів користувачів для яких виконується шифрування будуть відрізнятись від параметрів ключів користувача що виконує шифрування, користувачу буде видане повідомлення про неможливість виконування шифрування у зв’язку з відмінністю параметрів та процес шифрування буде припинено. Для запобігання цього слід переглянути сертифікат користувача на адресу якого виконується шифрування та перевірити відповідність параметрів власних ключів параметрам ключів цього користувача.

Після здійснення зашифрування файлів буде виведене наступне вікно (рис. 5.8) з інформацією про результати зашифрування.

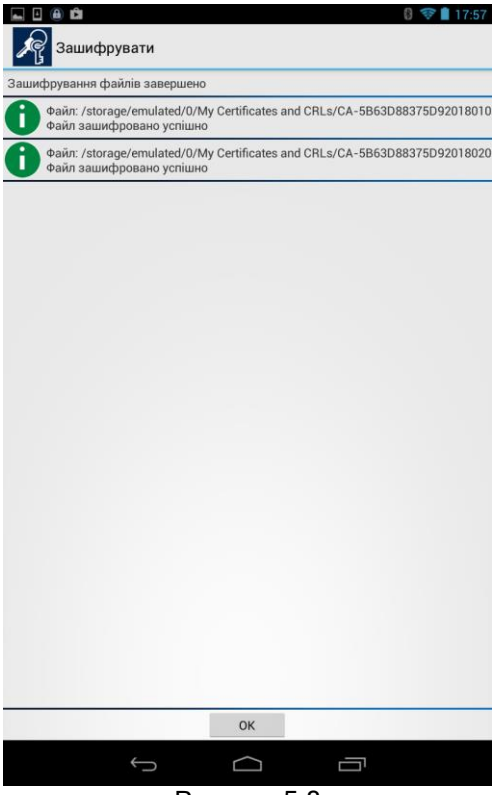

Рисунок 5.8

5.4 Розшифрування файлів

Для розшифрування файлів необхідно обрати пункт меню “Розшифрувати” (рис. 3.1). Якщо особистий ключ ще не було зчитано, відбувається його зчитування відповідно до п. 4.2.

Вікно розшифрування файлів наведене на рис. 5.9. Вікно містить список файлів. Файли, які можуть бути розшифровані мають розширення “.p7e”. Кнопка з зображенням синьої стрілки використовується для пересування до каталогу на рівень вище.

Файли для розшифрування обираються за допомогою торкання екрану пристрою напроти необхідного файлу. Для скасування розшифрування необхідно повторно торкнутися екрану пристрою напроти необхідного файлу (рис. 5.9).

Рисунок 5.9

Для розшифрування файлів необхідно натиснути кнопку “OK”. Після розшифрування буде виведено інформацію про результати розшифрування (рис. 5.10).

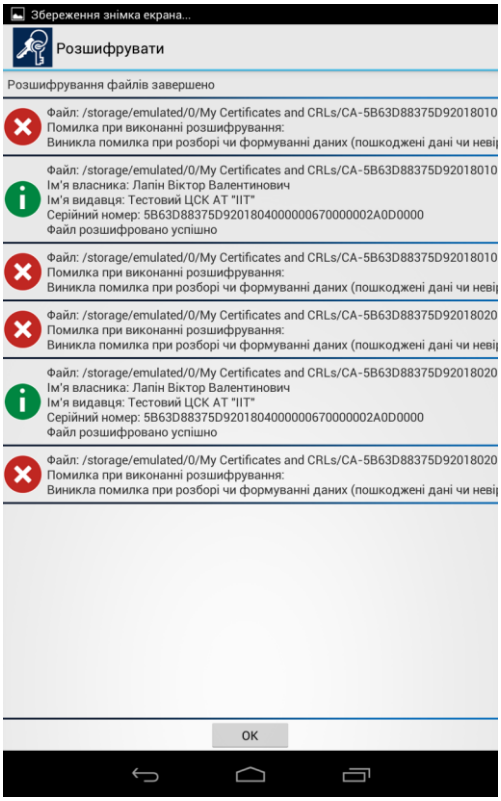

Рисунок 5.10

В разі вдалого розшифрування є можливість переглянути інформацію про сертифікат користувача, який зашифрував файл (рис. 5.11), для чого необхідно натиснути на запис про відповідний файл.

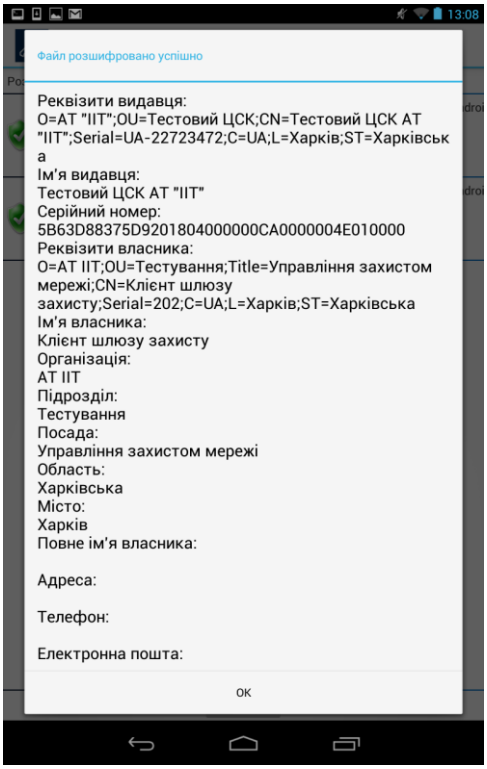

Рисунок 5.11

Розшифровані файли будуть записані до того ж каталогу у якому знаходилися зашифровані.

6 ЗАХИСТ ТЕКСТОВИХ ПОВІДОМЛЕНЬ

6.1 Зашифрування текстових повідомлень

Для зашифрування текстових повідомлень необхідно обрати пункт меню “Зашифрувати текст” (рис. 3.1). Якщо особистий ключ ще не було зчитано, відбувається його зчитування відповідно до п. 4.2.

Вікно зашифрування текстового повідомлення наведене на рис. 6.1. Вікно містить поле для введення тексту, який буде зашифровано. Кнопка з надписом “Зашифрувати” використовується для виконання зашифрування текстового повідомлення після завершення його введення.

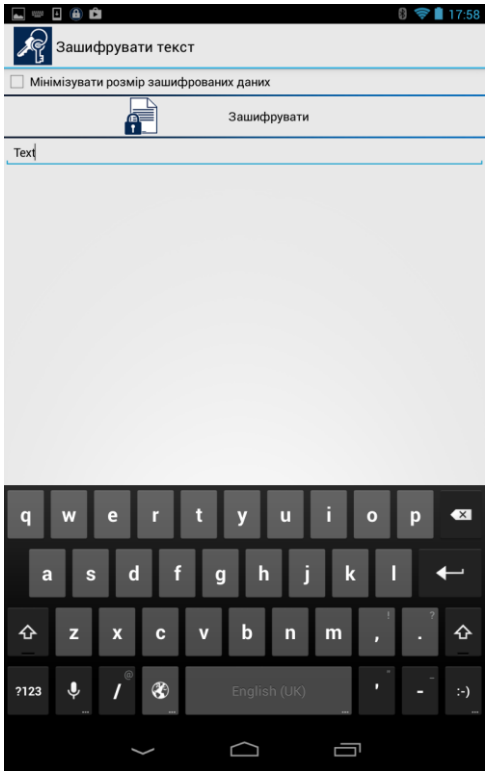

Рисунок 6.1

Для зашифрування текстового повідомлення використовується особистий ключ користувача що виконує зашифрування та сертифікат(и) користувача(ів) для якого(их) зашифровується файл. Тому у вікні що наведене на рис. 6.2 необхідно обрати сертифікати користувачів для яких виконується зашифрування тексту. Зашифрований текст може бути відкритим лише користувачем для якого виконувалось зашифрування.

Після завершення зашифрування текстового повідомлення буде запропоновано відправити зашифроване повідомлення за допомогою вбудованого акаунта Gmail засобами ОС Android (рис. 6.3).

Після обрання ікони Gmail буде відкрито вікно Gmail клієнта ОС Android, наведене на рис. 6.4. У графі “Кому” треба ввести електронну адресу отримувача зашифрованого текстового повідомлення, та натиснути кнопку “Надіслати”.

Рисунок 6.2

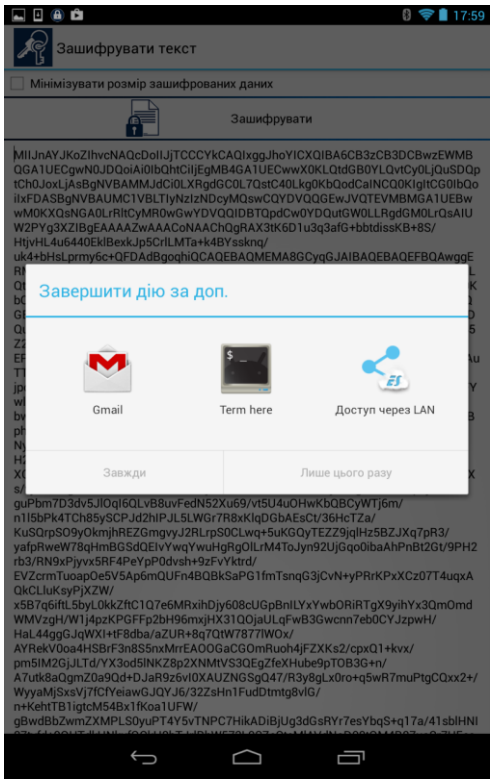

Рисунок 6.3

Пор. № зміни	Підпис відпов. особи	Дата внесення

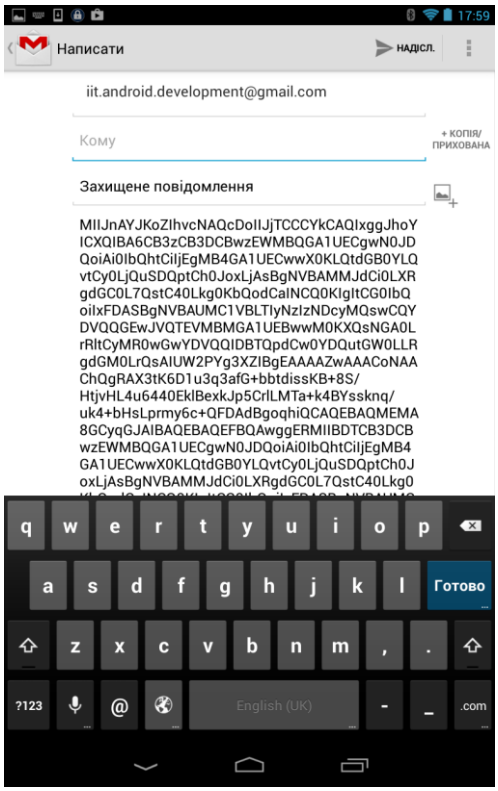

Рисунок 6.4

6.2 Розшифрування текстових повідомлень

Для розшифрування текстових повідомлень необхідно обрати пункт меню “Розшифрувати текст” (рис. 3.1). Якщо особистий ключ ще не було зчитано, відбувається його зчитування відповідно до п. 4.2.

Вікно розшифрування текстового повідомлення наведене на рис. 6.5. Вікно містить поле для введення зашифрованого тексту, це можна зробити за допомогою операції копіювання через буфер обміну. Кнопка з надписом “Розшифрувати” використовується для виконання розшифрування зашифрованого текстового повідомлення.

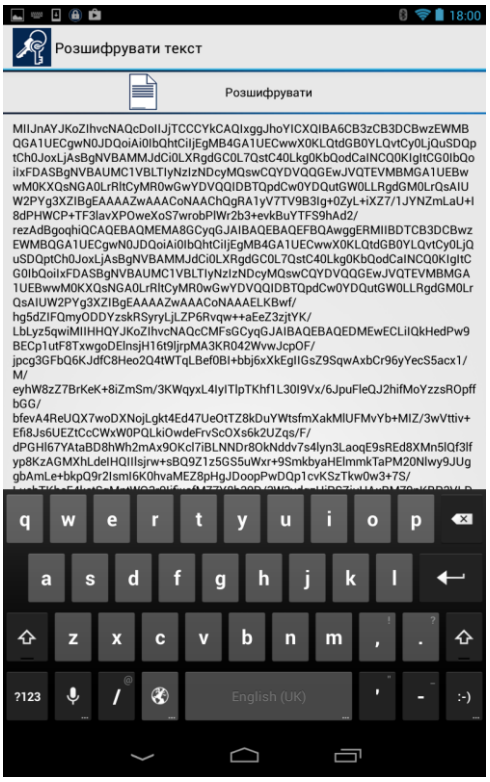

Рисунок 6.5

Вікно після виконання розшифрування зашифрованого текстового повідомлення наведене на рис. 6.6.

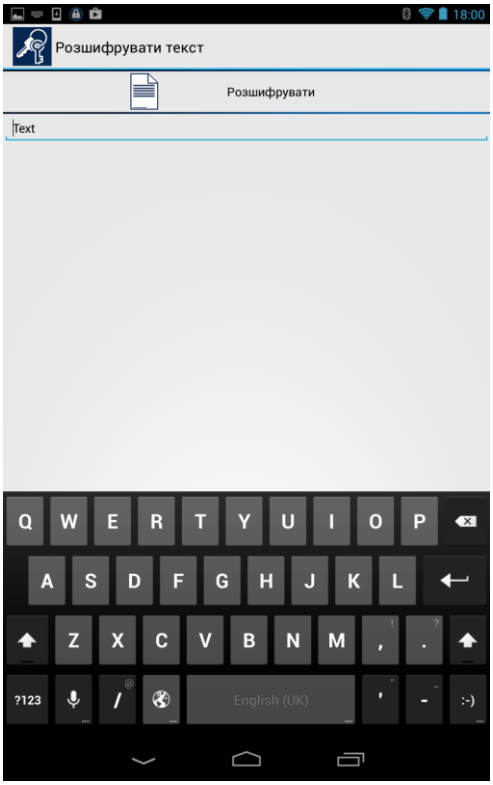

Рисунок 6.6

Пор. № зміни	Підпис відпов. особи	Дата внесення

ПЕРЕЛІК СКОРОЧЕНЬ

ОС	Операційна система
ЕЦП	Електронний цифровий підпис
КЗІ	Криптографічний захист інформації
ДКЕ	Довгостроковий ключовий елемент
СВС	Список відкликаних сертифікатів
ЦСК	Центр сертифікації ключів
НКІ	Носій ключової інформації (особистого ключа)
ПЕОМ	Персональна електронно-обчислювальна машина
CMP	Certificate Management Protocol (протокол управління обслуговуванням сертифікатів)
OCSP	Online Certificate Status Protocol (протокол визначення статусу сертифіката)
LDAP	Lightweight Directory Access Protocol (протокол доступу до каталогу)
TSP	Time-Stamp Protocol (протокол отримання позначок часу)
HTTP	Hyper Text Transfer Protocol