Program je možné spustiť na operačných systémoch Linux a Windows.

Potrebná knižnica pre spustenie programu je *cryptography* (https://pypi.org/project/cryptography/) a najnižšia potrebná verzia pythonu je *verzia 3.7.0*

Inštrukcie k spustenie program:

1. Spustiť súbor *source/CA.py* v príkazovom riadku
2. Zvoliť si číslo portu na ktorom bude tento program poslúchať pre komunikáciu od užívateľov, je nutne si zvoliť port viacej ako 1024 a menej ako 65536 ako napríklad 3333, po zadaní portu bude program iba vypisovať informácie a nie je potrebný ďalší input od užívateľa
3. Spustiť súbor *soruce/User.py* dva krát v **dvoch** rozdielnych príkazových riadkoch
4. Po spustení programov je potrebne si zvoliť dve rôzne mená (napr. Alice, Bob)
5. Zadať do programov číslo portu ktoré sme si zvolili ako port na ktorom bude CA čakať na komunikáciu (v tomto prípade 3333)
6. Teraz si zvolíme ktorý z používateľov začne výmenu certifikátov a zdieľanie AES kľúča, ako prvé je potrebne si zvoliť možnosť *receive* u jedného používateľa a potom až zvoliť *send* u druhého používateľa:
    a. **receive** – je potrebne si zvoliť port na ktorom bude používateľ poslúchať, rozsah zvoleného porta je 1024 – 65536 a port nesmie byt taký istý aký bol zvolený na začiatku pre certifikačnú autoritu (v tomto prípade 3333) takže napríklad port 4444
    b. **send** – je potrebné zvoliť port ktorý sme zvolili pri prvom používateľovi (v tomto prípade 4444)
7. Zase je možné si zvoliť ktorý z užívateľov bude posielať správu a ktorý bude primať správu (send/receive/quit)
    a. **send** – požívateľ zadá správu ktorú chce zadať priamo alebo súbor nasledovným formátom : **file:***absolútna_cesta_súboru* (napr. file:C:\test.txt)
    b. **receive** – používateľ si môže zvoliť ak bude primať správu ako len reťazec znakov ktorý bude vypísaný do konzole alebo zapísať správu do súboru takým istým formátom ako pri posielaní súboru, súbor do ktorého sa bude zapisovať správa nemusí byt vytvorený ale proces musí mat správne oprávnenia na zapisovanie do súboru, ak je v súboru už niečo zapísane proces vymaže pôvodný obsah súboru. Taktiež náš program dokáže posielať súbory len vo formáte .txt ,ak používateľ chce primať správu bez zapisovania do súboru stačí zadať “no”
    c. **quit** – program sa zastaví
8. Ďalej si môžu užívatelia vymieňať správy až kým platnosť certifikátu nevyprší
9. Po skončení program sa v zložke *certs* objavia 3 súbory v ktorých budú uložene certifikáty pre všetkých užívateľov a certifikačnú autority