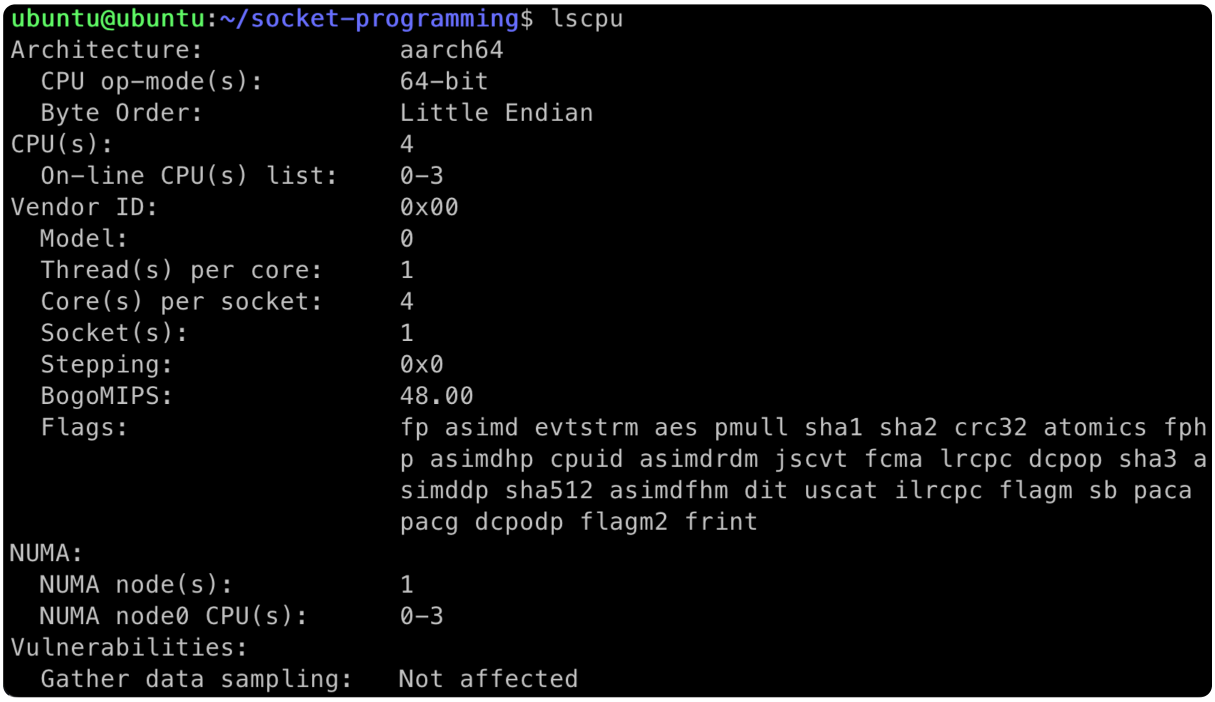
Socket Programming - SSL

Author: B12705014 陳泊華

操作說明

- 執行環境：Mac m1 UTM 開啟 Ubuntu22.04 VM



```
ubuntu@ubuntu:~/socket-programming$ lscpu
Architecture:            aarch64
  CPU op-mode(s):        64-bit
  Byte Order:            Little Endian
CPU(s):                  4
  On-line CPU(s) list:   0-3
Vendor ID:               0x00
  Model:                 0
  Thread(s) per core:    1
  Core(s) per socket:    4
  Socket(s):             1
  Stepping:              0x0
  BogoMIPS:              48.00
  Flags:                 fp asimd evtstrm aes pmull sha1 sha2 crc32 atomics fph
                         p asimdhp cpuid asimdrdm jscvt fcma lrcpc dcpop sha3 a
                         simddp sha512 asimdfhm dit uscat ilrcpc flagm sb paca
                         pacg dcpodp flagm2 frint
NUMA:
  NUMA node(s):          1
  NUMA node0 CPU(s):     0-3
Vulnerabilities:
  Gather data sampling:  Not affected
```

- 編譯指令：

  `g++ -std=c++17 -o client4 client4.cpp -lstdc++fs -lssl -lcrypto`

  `g++ -std=c++17 -o client4 client4.cpp -lstdc++fs -lssl -lcrypto`

- 執行指令：

  `./server8_ssl 8888 -a`

  `./client8_ssl 127.0.0.1 8888`

參考資料

- openssl http://jianiau.blogspot.com/2015/07/openssl-generating-rsa-key.html (http://jianiau.blogspot.com/2015/07/openssl-generating-rsa-key.html)
- BIO vs. PEM format https://stackoverflow.com/questions/30225782/how-to-read-a-public-key-from-a-pem-file-using-bio-from-openssl

(https://stackoverflow.com/questions/30225782/how-to-read-a-public-key-from-a-pem-file-using-bio-from-openssl)

Exception Handling:

1. 轉帳超過額度上限則返回目錄
2. login的username不能亂輸入（安全考量，如使用者輸入#之類的符號）
3. 轉帳時檢查payee是否存在；沒有就回傳找不到target payee然後返回目錄
4. 以上幾點同之前server和client程式，而此處多出檢查public key, private key是否存在，若不存在才進行key generate