

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO THỰC HÀNH  
HỌC PHẦN: MẬT MÃ HỌC CƠ SỞ  
MÃ HỌC PHẦN: INT1344**

**BÀI THỰC HÀNH:  
Cài đặt và cấu hình CA Server**

Sinh viên thực hiện:

Nguyễn Văn Hùng - B22DCAT136

Giảng viên hướng dẫn: TS. Quản Trọng Thế

**HÀ NỘI 5-2025**

# MỤC LỤC

MỤC LỤC .....	1
DANH MỤC CÁC HÌNH VẼ .....	2
DANH MỤC CÁC BẢNG BIỂU .....	2
DANH MỤC CÁC TỪ VIẾT TẮT .....	3
CHƯƠNG 1. Giới thiệu chung về bài thực hành .....	4
1.1 Mục đích .....	4
1.2 Giới thiệu chung .....	4
1.3 Tìm hiểu lý thuyết .....	4
1.3.1 Tổng quan .....	4
1.3.2 Quy trình hoạt động .....	5
1.3.3 Cơ chế bảo mật .....	5
1.3.4 Lợi ích và hạn chế cần lưu ý .....	5
1.4 Kết chương .....	6
CHƯƠNG 2. Nội dung thực hành .....	7
2.1 Chuẩn bị môi trường .....	7
2.2 Các bước thực hiện .....	7
2.2.1 Cấu hình và cài đặt môi trường CA Server .....	7
2.2.2 Tạo yêu cầu ký chứng chỉ .....	11
CHƯƠNG 3. Kết quả .....	14
TÀI LIỆU THAM KHẢO .....	15

## **DANH MỤC CÁC HÌNH VẼ**

Hình 1 . Khởi động bài lab .....	7
Hình 2 . Tạo thư mục easy-rsa và liên kết .....	8
Hình 3 . Cấp quyền và khởi tạo PKI .....	8
Hình 4 . Tạo CA .....	9
Hình 5 . Xem nội dung chứng chỉ CA .....	10
Hình 6 . Nhập chứng chỉ vào hệ thống client .....	10
Hình 7 . Tạo private key .....	11
Hình 8 . Tạo CSR .....	11
Hình 9 . Ký chứng chỉ .....	12
Hình 10 . Gửi chứng chỉ đã ký về client .....	13
Hình 11 . Kết quả bài lab .....	14

## **DANH MỤC CÁC BẢNG BIỂU**

Bảng 1. Cơ chế bảo mật .....	5
------------------------------	---

## DANH MỤC CÁC TỪ VIẾT TẮT

<b>Từ viết tắt</b>	<b>Thuật ngữ tiếng Anh/Giải thích</b>	<b>Thuật ngữ tiếng Việt/Giải thích</b>
CA	Certificate Authority	Cơ quan chứng nhận/Cơ quan cấp chứng chỉ
PKI	Public Key Infrastructure	Hạ tầng khóa công khai
CSR	Certificate Signing Request	Yêu cầu ký chứng chỉ
TLS	Transport Layer Security	Bảo mật tầng giao vận
HTTPS	Hypertext Transfer Protocol Secure	Giao thức truyền tải siêu văn bản an toàn
CRL	Certificate Revocation List	Danh sách thu hồi chứng chỉ
OCSP	Online Certificate Status Protocol	Giao thức kiểm tra trạng thái chứng chỉ trực tuyến
ECC	Elliptic Curve Cryptography	Mật mã đường cong elliptic
RSA	Rivest–Shamir–Adleman	Thuật toán mã hóa RSA
MITM	Man-in-the-Middle Attack	Tấn công nghe lén trung gian
HSM	Hardware Security Module	Mô-đun bảo mật phần cứng

# CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

## 1.1 Mục đích

- Chúng ta sẽ tìm hiểu cách thiết lập CA server trên máy chủ Ubuntu cũng như cách tạo và ký chứng chỉ kiểm tra bằng CA mới
- Chúng ta cũng sẽ tìm hiểu cách nhập chứng chỉ công khai của máy chủ CA vào kho chứng chỉ của hệ điều hành để có thể xác minh chuỗi tin cậy giữa CA và máy chủ hoặc người dùng từ xa.

## 1.2 Giới thiệu chung

Certificate Authority (CA) là một tổ chức chịu trách nhiệm cấp chứng chỉ số để xác minh danh tính trên internet. Trong khi các CA công cộng thường được sử dụng để xác thực danh tính của các trang web và dịch vụ cho công chúng, thì các CA riêng tư thường được dùng trong các nhóm kín và các dịch vụ nội bộ.

Việc xây dựng một Certificate Authority (CA) riêng cho phép sinh viên cấu hình, kiểm tra và vận hành các chương trình yêu cầu kết nối được mã hóa giữa máy khách và máy chủ. Với một CA riêng, sinh viên có thể cấp chứng chỉ cho người dùng, máy chủ, hoặc các chương trình và dịch vụ cụ thể trong hệ thống của mình.

Một số ví dụ về các chương trình Linux sử dụng CA riêng bao gồm OpenVPN và Puppet. Sinh viên cũng có thể cấu hình máy chủ web sử dụng chứng chỉ do CA riêng cấp để phát triển hoặc kiểm thử, đảm bảo các môi trường giống như máy chủ sản xuất sử dụng TLS để mã hóa kết nối.

Trong bài thực hành cấu hình CA này sinh viên sẽ được tự tay cấu hình CA riêng của riêng mình được sử dụng trong nội bộ. Sinh viên tự thực hiện cấu hình trên ubuntu, thực hiện tạo yêu cầu chứng chỉ. Qua bài thực hành sinh viên sẽ hiểu cách mà một CA server hoạt động, hiểu được cách tạo 1 yêu cầu và cách CA xác nhận yêu cầu đó. Điều đó cho sinh viên cái nhìn tốt hơn về việc CA server hoạt động và phát triển tốt hơn trong lĩnh vực an toàn thông tin

## 1.3 Tìm hiểu lý thuyết

### 1.3.1 Tổng quan

PKI (Public Key Infrastructure) là hệ thống quản lý khóa công khai và chứng chỉ số, đảm bảo tính xác thực, bảo mật và toàn vẹn dữ liệu trong giao tiếp mạng.

Certificate Authority (CA) đóng vai trò là trung tâm tin cậy, chịu trách nhiệm:

- Tạo và ký chứng chỉ số (digital certificates).
- Xác minh danh tính của các thực thể (máy chủ, người dùng).
- Quản lý vòng đời chứng chỉ (tạo, ký, thu hồi).

### 1.3.2 Quy trình hoạt động

#### 1.3.2.1 Thiết lập Root CA

- Khởi tạo PKI: Tạo cấu trúc thư mục lưu trữ khóa/chứng chỉ.
- Tạo Root Certificate:
  - o Sinh cặp khóa RSA/ECC cho CA.
  - o Tự ký chứng chỉ gốc (self-signed certificate).
- Phân phối CA Certificate: Sao chép ca.crt đến các client để thiết lập niềm tin.

#### 1.3.2.2 Tạo và ký chứng chỉ

- Client tạo CSR: `openssl req -new -key client.key -out client.req`
- CA ký chứng chỉ: `./easysrsa sign-req server client_name`
  - o Xác minh CSR.
  - o Thêm chữ ký số bằng CA private key.
  - o Đính kèm thông tin CA vào chứng chỉ.

#### 1.3.2.3 Triển khai chứng chỉ

Client sử dụng chứng chỉ đã ký (client.crt) cùng private key để:

- Cấu hình HTTPS trên web server.
- Thiết lập VPN (OpenVPN).
- Xác thực trong các dịch vụ nội bộ.

### 1.3.3 Cơ chế bảo mật

Bảng 1. Cơ chế bảo mật

Cơ chế	Mô tả
Chain of Trust	Client tin cậy chứng chỉ server vì nó được ký bởi CA đã được import
Private Key Protection	CA private key được bảo vệ bằng passphrase và lưu trữ offline
Certificate Revocation	CRL (Certificate Revocation List) hoặc OCSP để thu hồi chứng chỉ

#### 1.3.4 Lợi ích và hạn chế cần lưu ý

Lợi ích của CA riêng:

- Toàn quyền kiểm soát: Tự quản lý vòng đời chứng chỉ.
- Tiết kiệm chi phí: Không cần mua chứng chỉ thương mại cho mục đích nội bộ.

- Tùy chỉnh linh hoạt: Đặt các chính sách riêng (key length, thuật toán, validity period).

Hạn chế cần lưu ý:

- Quản lý khóa gốc: Nếu CA private key bị lộ, toàn bộ hệ thống mất an toàn.
- Phân phối chứng chỉ gốc: Client phải cài đặt thủ công ca.crt.
- Không dùng cho public-facing services: Trình duyệt/web client không tin cậy CA tự tạo.

#### **1.4 Kết chương**

Bài thực hành cung cấp nền tảng để hiểu cách vận hành PKI và CA riêng. Qua đó, sinh viên có thể nắm rõ cơ chế mã hóa, xác thực và quản lý rủi ro trong an toàn thông tin.

## CHƯƠNG 2. NỘI DUNG THỰC HÀNH

### 2.1 Chuẩn bị môi trường

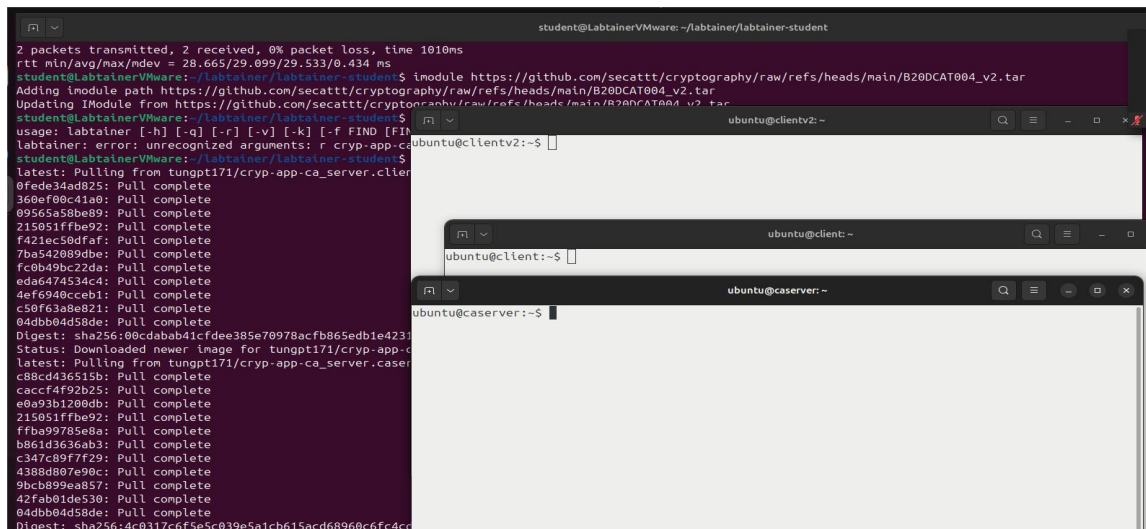
- Phần mềm ảo hóa VMWare Workstation
- Máy ảo Labtainer

### 2.2 Các bước thực hiện

#### 2.2.1 Cấu hình và cài đặt môi trường CA Server

##### 2.2.1.1 Chuẩn bị môi trường PKI

Khởi động bài lab: `labtainer -r cryp-app-ca_server`



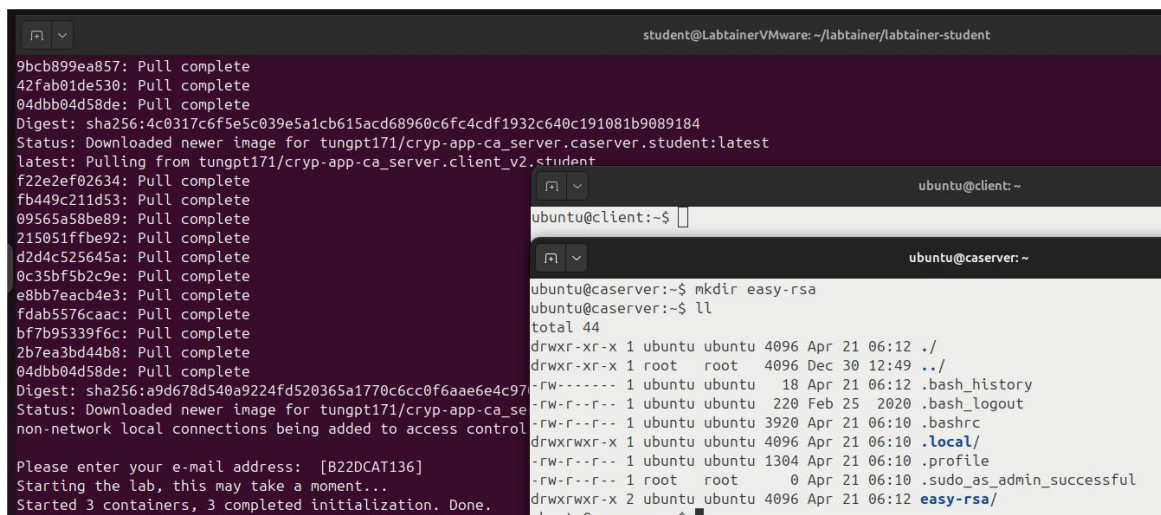
Hình 1. Khởi động bài lab

Nhập email là mã sinh viên: `B22DCAT136`

Trên terminal caserver, tạo thư mục easy-rsa và liên kết:

`mkdir easy-rsa`

`ln -s /usr/share/easy-rsa/* easy-rsa/`





```
ubuntu@caserver:~$ mkdir easy-rsa
ubuntu@caserver:~$ ll
total 44
drwxr-xr-x 1 ubuntu ubuntu 4096 Apr 21 06:12 ./
drwxr-xr-x 1 root root 4096 Dec 30 12:49 ../
-rw-r--r-- 1 ubuntu ubuntu 18 Apr 21 06:12 .bash_history
-rw-r--r-- 1 ubuntu ubuntu 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3920 Apr 21 06:10 .bashrc
drwxrwxr-x 1 ubuntu ubuntu 4096 Apr 21 06:10 .local/
-rw-r--r-- 1 ubuntu ubuntu 1304 Apr 21 06:10 .profile
-rw-r--r-- 1 root root 0 Apr 21 06:10 .sudo_as_admin_successful
drwxrwxr-x 2 ubuntu ubuntu 4096 Apr 21 06:12 easy-rsa/
ubuntu@caserver:~$ ln -s /usr/share/easy-rsa/* easy-rsa/
ubuntu@caserver:~$ pwd
/home/ubuntu
ubuntu@caserver:~$ chmod 700 /home/ubuntu/easy-rsa
ubuntu@caserver:~$ ll
total 44
drwxr-xr-x 1 ubuntu ubuntu 4096 Apr 21 06:12 ./
drwxr-xr-x 1 root root 4096 Dec 30 12:49 ../
-rw-r--r-- 1 ubuntu ubuntu 95 Apr 21 06:14 .bash_history
-rw-r--r-- 1 ubuntu ubuntu 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3920 Apr 21 06:10 .bashrc
drwxrwxr-x 1 ubuntu ubuntu 4096 Apr 21 06:10 .local/
-rw-r--r-- 1 ubuntu ubuntu 1304 Apr 21 06:10 .profile
-rw-r--r-- 1 root root 0 Apr 21 06:10 .sudo_as_admin_successful
drwx----- 2 ubuntu ubuntu 4096 Apr 21 06:13 easy-rsa/
ubuntu@caserver:~$
```

Hình 2. Tạo thư mục easy-rsa và liên kết

Cấp quyền thư mục PKI (easy-rsa):

*chmod 700 /home/ubuntu/easy-rsa*

*cd easy-rsa*

*./easysrsa init-pki*

```
ubuntu@caserver:~/easy-rsa$ chmod 700 /home/ubuntu/easy-rsa
ubuntu@caserver:~/easy-rsa$ ll
total 44
drwxr-xr-x 1 ubuntu ubuntu 4096 Apr 21 06:12 ./
drwxr-xr-x 1 root root 4096 Dec 30 12:49 ../
-rw-r--r-- 1 ubuntu ubuntu 95 Apr 21 06:14 .bash_history
-rw-r--r-- 1 ubuntu ubuntu 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3920 Apr 21 06:10 .bashrc
drwxrwxr-x 1 ubuntu ubuntu 4096 Apr 21 06:10 .local/
-rw-r--r-- 1 ubuntu ubuntu 1304 Apr 21 06:10 .profile
-rw-r--r-- 1 root root 0 Apr 21 06:10 .sudo_as_admin_successful
drwx----- 2 ubuntu ubuntu 4096 Apr 21 06:13 easy-rsa/
ubuntu@caserver:~/easy-rsa$ cd easy-rsa
ubuntu@caserver:~/easy-rsa$ ll
total 12
drwx----- 2 ubuntu ubuntu 4096 Apr 21 06:13 ./
drwxr-xr-x 1 ubuntu ubuntu 4096 Apr 21 06:12 ../
lrwxrwxrwx 1 ubuntu ubuntu 27 Apr 21 06:13 easysrsa -> /usr/share/easy-rsa/easysrsa*
lrwxrwxrwx 1 ubuntu ubuntu 39 Apr 21 06:13 openssl-easysrsa.cnf -> /usr/share/easy-rsa/openssl-easy
rsa.cnf
lrwxrwxrwx 1 ubuntu ubuntu 32 Apr 21 06:13 vars.example -> /usr/share/easy-rsa/vars.example
lrwxrwxrwx 1 ubuntu ubuntu 30 Apr 21 06:13 x509-types -> /usr/share/easy-rsa/x509-types/
ubuntu@caserver:~/easy-rsa$ ./easysrsa init-pki

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /home/ubuntu/easy-rsa/pki
```

Hình 3. Cấp quyền và khởi tạo PKI

### 2.2.1.2 Tạo Certificate Authority

Tạo file vars: *nano vars*

Lưu thông tin:

```

set_var EASYRSA_REQ_COUNTRY    "VN"
set_var EASYRSA_REQ_PROVINCE   "Hanoi"
set_var EASYRSA_REQ_CITY       "Hanoi City"
set_var EASYRSA_REQ_ORG        "none"
set_var EASYRSA_REQ_EMAIL      "admin@example.com"
set_var EASYRSA_REQ_OU         "Community"
set_var EASYRSA_ALGO           "ec"
set_var EASYRSA_DIGEST         "sha512"

```

Xây dựng CA: `./easyrsa build-ca`

- Nhập CA Key Passphrase
- Nhập Common Name hoặc có thể để mặc định

The image consists of two screenshots of a terminal window. The top screenshot shows the contents of the `vars` file in the `easy-rsa` directory, where various configuration variables are set, including country, province, city, organization, email, OU, algorithm, and digest. The bottom screenshot shows the execution of the `./easyrsa build-ca` command. It displays the EasyRSA configuration being used, the OpenSSL version and date, and prompts for a new CA key passphrase and a new CA key. It then shows an error message about a random number generator, followed by a prompt to enter information for the certificate request, specifically the Common Name (CN).

```

ubuntu@caserver: ~/easy-rsa
GNU nano 4.8 vars
set_var EASYRSA_REQ_COUNTRY    "VN"
set_var EASYRSA_REQ_PROVINCE   "Hanoi"
set_var EASYRSA_REQ_CITY       "Hanoi City"
set_var EASYRSA_REQ_ORG        "none"
set_var EASYRSA_REQ_EMAIL      "admin@example.com"
set_var EASYRSA_REQ_OU         "Community"
set_var EASYRSA_ALGO           "ec"
set_var EASYRSA_DIGEST         "sha512"

ubuntu@caserver: ~/easy-rsa
ubuntu@caserver:~/easy-rsa$ nano vars
ubuntu@caserver:~/easy-rsa$ ./easyrsa build-ca

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.1.1f  31 Mar 2020

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
read EC key
writing EC key
Can't load /home/ubuntu/easy-rsa/pki/.rnd into RNG
140044907255104:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:98
:Filename=/home/ubuntu/easy-rsa/pki/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/home/ubuntu/easy-rsa/pki/ca.crt

```

Hình 4. Tạo CA

### 2.2.1.3 Nhập chứng chỉ vào máy client

Xem nội dung chứng chỉ CA:

```
cd pki
```

*cat ca.crt*

```
ubuntu@caser: ~/easy-rsa/pki
-rw-rw-r-- 1 ubuntu ubuntu 327 Apr 21 06:19 vars
lrwxrwxrwx 1 ubuntu ubuntu 32 Apr 21 06:13 vars.example -> /usr/share/easy-rsa/vars.example
lrwxrwxrwx 1 ubuntu ubuntu 30 Apr 21 06:13 x509-types -> /usr/share/easy-rsa/x509-types/
ubuntu@caser: ~/easy-rsa$ cd pki
ubuntu@caser: ~/easy-rsa/pki$ ll
total 64
drwx----- 9 ubuntu ubuntu 4096 Apr 21 06:25 ./
drwx----- 3 ubuntu ubuntu 4096 Apr 21 06:23 ../
-rw----- 1 ubuntu ubuntu 1024 Apr 21 06:25 .rnd
-rw----- 1 ubuntu ubuntu 749 Apr 21 06:25 ca.crt
drwx----- 2 ubuntu ubuntu 4096 Apr 21 06:20 certs_by_serial/
drwx----- 2 ubuntu ubuntu 4096 Apr 21 06:20 ecparams/
-rw----- 1 ubuntu ubuntu 0 Apr 21 06:23 index.txt
drwx----- 2 ubuntu ubuntu 4096 Apr 21 06:20 issued/
-rw----- 1 ubuntu ubuntu 4651 Apr 21 06:15 openssl-easyrsa.cnf
drwx----- 2 ubuntu ubuntu 4096 Apr 21 06:25 private/
drwx----- 5 ubuntu ubuntu 4096 Apr 21 06:20 renewed/
drwx----- 2 ubuntu ubuntu 4096 Apr 21 06:15 reqs/
drwx----- 5 ubuntu ubuntu 4096 Apr 21 06:20 revoked/
-rw----- 1 ubuntu ubuntu 4653 Apr 21 06:24 safessl-easyrsa.cnf
-rw----- 1 ubuntu ubuntu 3 Apr 21 06:23 serial
ubuntu@caser: ~/easy-rsa/pki$ cat ca.crt
-----BEGIN CERTIFICATE-----
MIIB+zCCAYKgAwIBAgIUd9xJhGh+jSG89jk1t5QSddqia18wCgYIKoZIzj0EAwQw
FjEUMBIGA1UEAwLRWFZeS1SU0EgQ0EwHcNMjUwNDIxMDYyNTA4WmcNMzUwNDU5
MDYyNTA4WjAAMRQwEgYDVQDDAtFYXN5LVJTSBDBQTB2MBAGByqGSM49AgEGBSuB
BAAIA2IABJLQycdOWnxYHicJDax+ASrTSgZHjRMuvLOZbyWnFz+4SGsyvO2ICxU3
awLn5KAKY7GnAgR285AoLesCoQsBu9OWRxpPa1yUq8C6sBgsX+WfZQsWEUSaGdIB
ZeGukoVsqOBkDCBjTAdBgNVHQ4EFgQUSlQtKxiGTW6PnmWJCegjKk58RdEwUQYD
VR0jBEowSIAUSlQtKxiGTW6PnmWJCegjKk58RdGhGqQYMBYxFDASBgNVBAMMC0Vh
c3ktU1NBIEBghQP3EmEaH6NIbz20TW3lBj12qJrXzAMBGNVHRMEBTADAQH/MASG
A1UdDwQEAWIBBjAKBgqhkhjOPQDBANnADBKAjBpjoRim+iyLDNK4BPY+nyN7Of1
rh892F2ZTWszJleJewEE9CM6nx4gMEuJLyWB364CMFRM5Qcsyef6Ku42ewAa92VB
tcG8fpg8VB6dJQs4LrFgfS4NV5yO3At04WZ8TKr8A==
-----END CERTIFICATE-----
ubuntu@caser: ~/easy-rsa/pki$
```

Hình 5. Xem nội dung chứng chỉ CA

Copy toàn bộ nội dung từ -----BEGIN CERTIFICATE----- đến -----END CERTIFICATE-----

Trên client, dán nội dung đã copy vào /tmp/ca.crt: *nano /tmp/ca.crt*

Nhập chứng chỉ vào hệ thống:

*sudo cp /tmp/ca.crt /usr/local/share/ca-certificates/*

*sudo update-ca-certificates*

```
ubuntu@client: ~
ubuntu@client:~$ ll
total 44
drwxr-xr-x 1 ubuntu ubuntu 4096 Apr 21 06:34 ./
drwxr-xr-x 1 root root 4096 Dec 30 12:48 ../
-rw----- 1 ubuntu ubuntu 3 Apr 21 06:34 .bash_history
-rw-r--r-- 1 ubuntu ubuntu 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3920 Apr 21 06:10 .bashrc
-rw-r--r-- 1 ubuntu ubuntu 33 Apr 21 06:10 .hashrandom
drwxrwxr-x 1 ubuntu ubuntu 4096 Apr 21 06:22 .local/
-rw-r--r-- 1 ubuntu ubuntu 1304 Apr 21 06:10 .profile
-rw-r--r-- 1 root root 0 Apr 21 06:10 .sudo_as_admin_successful
ubuntu@client:~$ nano /tmp/ca.crt
ubuntu@client:~$ sudo cp /tmp/ca.crt /usr/local/share/ca-certificates/
ubuntu@client:~$ sudo update-ca-certificates
Updating certificates in /etc/ssl/certs...
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
ubuntu@client:~$
```

Hình 6. Nhập chứng chỉ vào hệ thống client



## 2.2.2 Tạo yêu cầu ký chứng chỉ

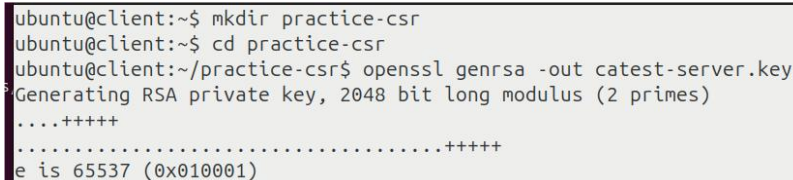
### 2.2.2.1 Tạo private key

Trên máy Client, tạo private key:

```
mkdir practice-csr
```

```
cd practice-csr
```

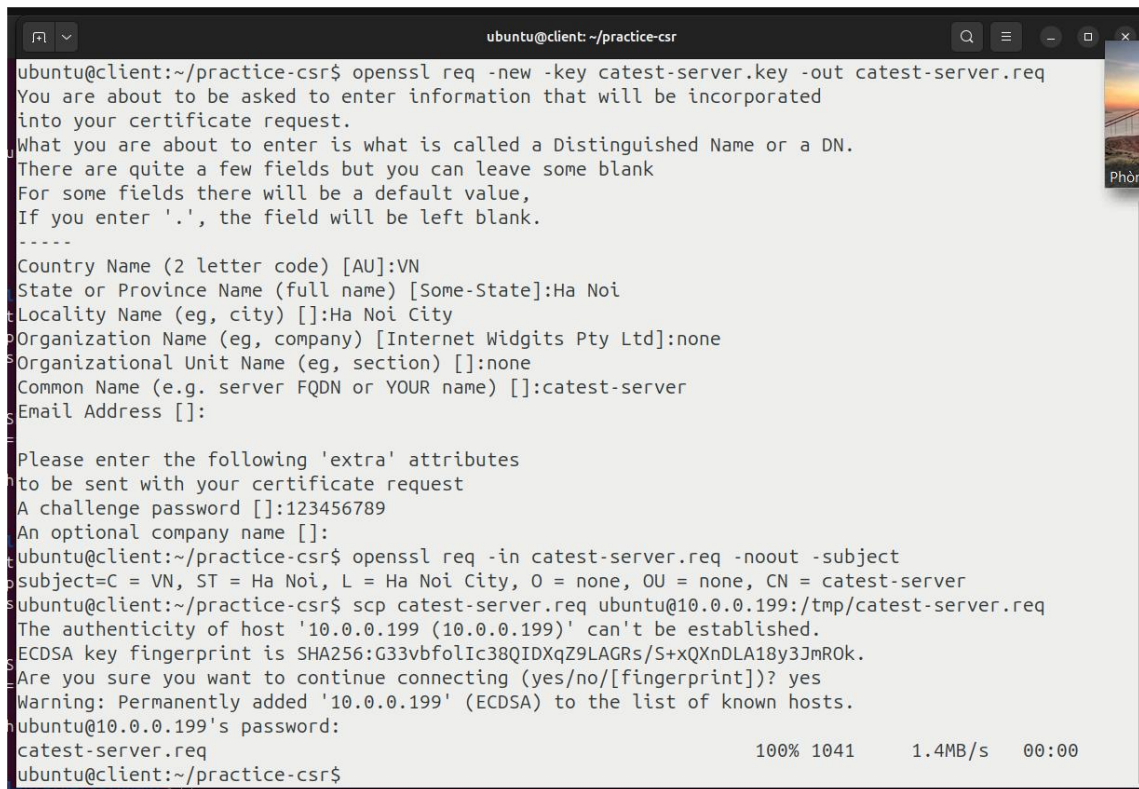
```
openssl genrsa -out catest-server.key
```



```
ubuntu@client:~$ mkdir practice-csr
ubuntu@client:~$ cd practice-csr
ubuntu@client:~/practice-csr$ openssl genrsa -out catest-server.key
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
```

Hình 7. Tạo private key

### 2.2.2.2 Tạo Certificate Signing Request (CSR)



```
ubuntu@client:~/practice-csr$ openssl req -new -key catest-server.key -out catest-server.req
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:VN
State or Province Name (full name) [Some-State]:Ha Noi
Locality Name (eg, city) []:Ha Noi City
Organization Name (eg, company) [Internet Widgits Pty Ltd]:none
Organizational Unit Name (eg, section) []:none
Common Name (e.g. server FQDN or YOUR name) []:catest-server
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456789
An optional company name []:
ubuntu@client:~/practice-csr$ openssl req -in catest-server.req -noout -subject
subject=C = VN, ST = Ha Noi, L = Ha Noi City, O = none, OU = none, CN = catest-server
ubuntu@client:~/practice-csr$ scp catest-server.req ubuntu@10.0.0.199:/tmp/catest-server.req
The authenticity of host '10.0.0.199 (10.0.0.199)' can't be established.
ECDSA key fingerprint is SHA256:G33vbf0Ic38QIDXqZ9LAGRs/S+XQXnDLA18y3JmR0k.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.199' (ECDSA) to the list of known hosts.
ubuntu@10.0.0.199's password:
catest-server.req                                     100% 1041      1.4MB/s   00:00
ubuntu@client:~/practice-csr$
```

Hình 8. Tạo CSR

Tạo CSR: *openssl req -new -key catest-server.key -out catest-server.req*

Nhập thông tin:

*Country Name: VN*

*State or Province Name: Ha Noi*

*Locality Name: Ha Noi City*

*Organization Name: none*

*Organizational Unit Name: none*

*Common Name: catest-server*

*Email Address: (bỏ trống)*

*Challenge password: 123456789 hoặc bỏ trống*

*Optional company name: (bỏ trống)*

Kiểm tra CSR: *openssl req -in catest-server.req -noout -subject*

Gửi CSR lên CA server:

*scp catest-server.req ubuntu@10.0.0.199:/tmp/catest-server.req*

Nhập mật khẩu khi được yêu cầu

### 2.2.2.3 Ký chứng chỉ

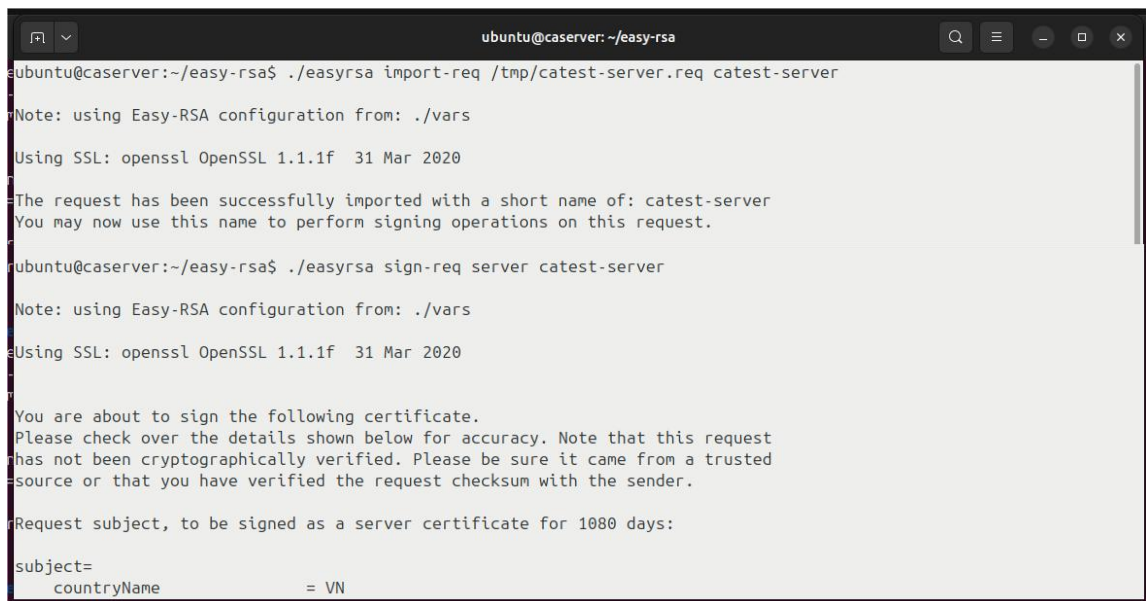
Trên caserver:

*cd easy-rsa*

*./easysrsa import-req /tmp/catest-server.req catest-server*

*./easysrsa sign-req server catest-server*

Nhập yes để xác nhận



```
ubuntu@caserver: ~/easy-rsa
ubuntu@caserver:~/easy-rsa$ ./easysrsa import-req /tmp/catest-server.req catest-server
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
The request has been successfully imported with a short name of: catest-server
You may now use this name to perform signing operations on this request.
ubuntu@caserver:~/easy-rsa$ ./easysrsa sign-req server catest-server
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1f 31 Mar 2020
You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.
Request subject, to be signed as a server certificate for 1080 days:
subject=
countryName = VN
```

Hình 9. Ký chứng chỉ

Gửi chứng chỉ đã ký về client:

*scp ubuntu@10.0.0.199:/home/ubuntu/easy-rsa/pki/issued/catest-server.crt /tmp*

*scp ubuntu@10.0.0.199:/home/ubuntu/easy-rsa/pki/ca.crt /tmp*

```
ubuntu@cserver: ~/easy-rsa

localityName           = Ha Noi City
organizationName       = none
organizationalUnitName = none
commonName             = catest-server

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
yes
Using configuration from /home/ubuntu/easy-rsa/pki/safessl-easyrsa.cnf
Enter pass phrase for /home/ubuntu/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'VN'
stateOrProvinceName     :ASN.1 12:'Ha Noi'
localityName            :ASN.1 12:'Ha Noi City'
organizationName        :ASN.1 12:'none'
organizationalUnitName  :ASN.1 12:'none'
commonName              :ASN.1 12:'catest-server'
Certificate is to be certified until Apr  5 06:49:00 2028 GMT (1080 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /home/ubuntu/easy-rsa/pki/issued/catest-server.crt

ubuntu@cserver:~/easy-rsa$ scp ubuntu@10.0.0.199:/home/ubuntu/easy-rsa/pki/issued/catest-server.crt /tmp
The authenticity of host '10.0.0.199 (10.0.0.199)' can't be established.
ECDSA key fingerprint is SHA256:G33vbfolic38QIDXqZ9LAGRs/S+xQXnDLA18y3JmROK.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.199' (ECDSA) to the list of known hosts.
ubuntu@10.0.0.199's password:
Permission denied, please try again.
ubuntu@10.0.0.199's password:
Connection closed by 10.0.0.199 port 22
ubuntu@cserver:~/easy-rsa$ scp ubuntu@10.0.0.199:/home/ubuntu/easy-rsa/pki/issued/catest-server.crt /tmp
ubuntu@10.0.0.199's password:
catest-server.crt                                100% 4017    2.3MB/s   00:00
ubuntu@cserver:~/easy-rsa$ scp ubuntu@10.0.0.199:/home/ubuntu/easy-rsa/pki/ca.crt /tmp
ubuntu@10.0.0.199's password:
ca.crt                                           100% 749    1.7MB/s   00:00
ubuntu@cserver:~/easy-rsa$
```

Hình 10. Gửi chứng chỉ đã ký về client

## CHƯƠNG 3. KẾT QUẢ

- Kết thúc bài lab: *stoplab*

```
student@LabtainerVMware: ~/labtainer/labtainer-student
Successfully copied 2.05kB to /home/student/labtainer_xfer/cryp-app-ca_server
Labname cryp-app-ca_server

Student | signingCSR | createPKI | createCA | addCA | createPriKey | createCSR |
===== | ===== | ===== | ===== | ===== | ===== | ===== |
B22DCAT136 | | Y | | | | |
What is automatically assessed for this lab:

student@LabtainerVMware:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/cryp-app-ca_server
Successfully copied 146kB to cryp-app-ca_server-igrader:/home/instructor/B22DCAT136.cryp-app-ca_server.lab
Successfully copied 2.05kB to /home/student/labtainer_xfer/cryp-app-ca_server
Labname cryp-app-ca_server

Student | signingCSR | createPKI | createCA | addCA | createPriKey | createCSR |
===== | ===== | ===== | ===== | ===== | ===== | ===== |
B22DCAT136 | | Y | Y | | | |
What is automatically assessed for this lab:

student@LabtainerVMware:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/cryp-app-ca_server
Successfully copied 162kB to cryp-app-ca_server-igrader:/home/instructor/B22DCAT136.cryp-app-ca_server.lab
Successfully copied 2.05kB to /home/student/labtainer_xfer/cryp-app-ca_server
Labname cryp-app-ca_server

Student | signingCSR | createPKI | createCA | addCA | createPriKey | createCSR |
===== | ===== | ===== | ===== | ===== | ===== | ===== |
B22DCAT136 | Y | Y | Y | Y | Y | Y |
What is automatically assessed for this lab:

student@LabtainerVMware:~/labtainer/labtainer-student$ stoplab
Results stored in directory: /home/student/labtainer_xfer/cryp-app-ca_server
student@LabtainerVMware:~/labtainer/labtainer-student$
```

Hình 11. Kết quả bài lab

- Khởi động lại lab nếu cần: *labtainer -r cryp-app-ca\_server*
- Kết quả bài lab được lưu: */home/student/labtainer\_xfer/cryp-app-ca\_server*

## TÀI LIỆU THAM KHẢO

- [1] <https://vietnix.vn/cach-thiet-lap-va-cau-hinh-certificate-authority-tren-ubuntu-20-04/>
- [2] <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf>