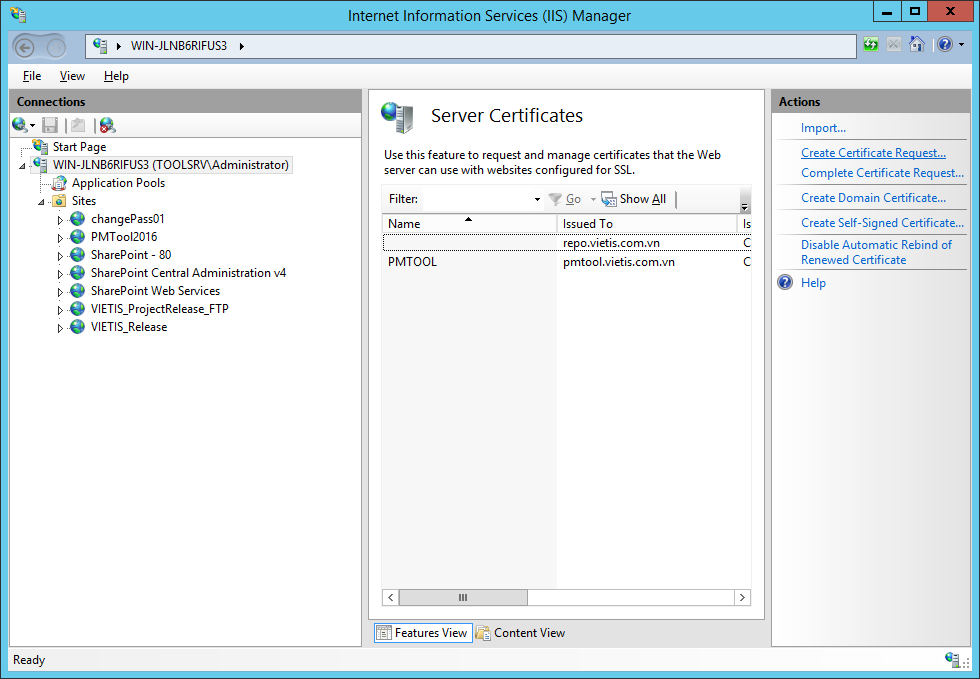
WINDOWS:

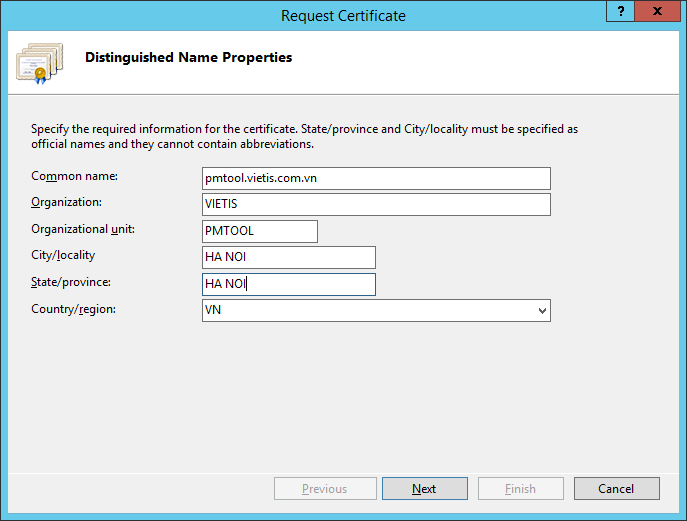
1. Tạo cer trong local windows:

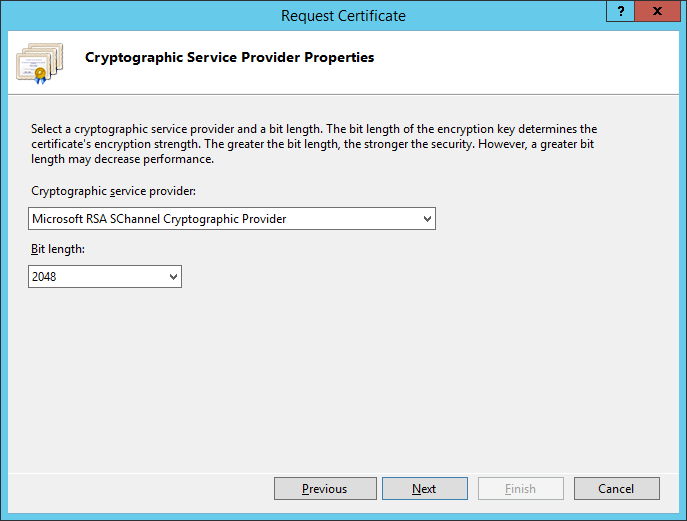
**Phải tạo cái này trên local con PMTOOL trước**

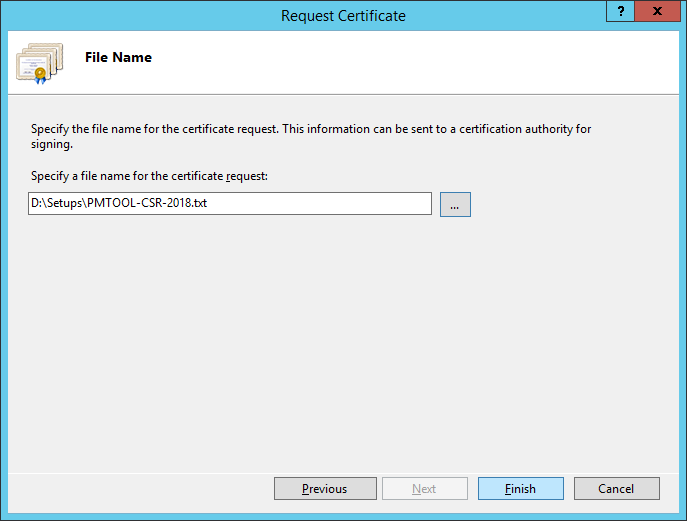
**insight.vietis.com.vn**

**Create Certificate Request**









1. Gửi cer lên trang ssl
2. Get KQ từ trang ssl

<https://baomat.website/huong-dan-chuyen-doi-ssl/huong-dan-import-pfx-vao-may-chu-windows-167.htm>

<http://www.stefanocapitanio.com/configuring-two-way-authentication-ssl-with-apache/>

<https://www.ssl.com/online-csr-and-key-generator/>

<https://csrgenerator.com/>

SSL Guideline

Em gửi anh thông tin quản lý SSL nhé.

**1/ Thông tin đăng nhập:**

URL: <https://www.ssls.com/>

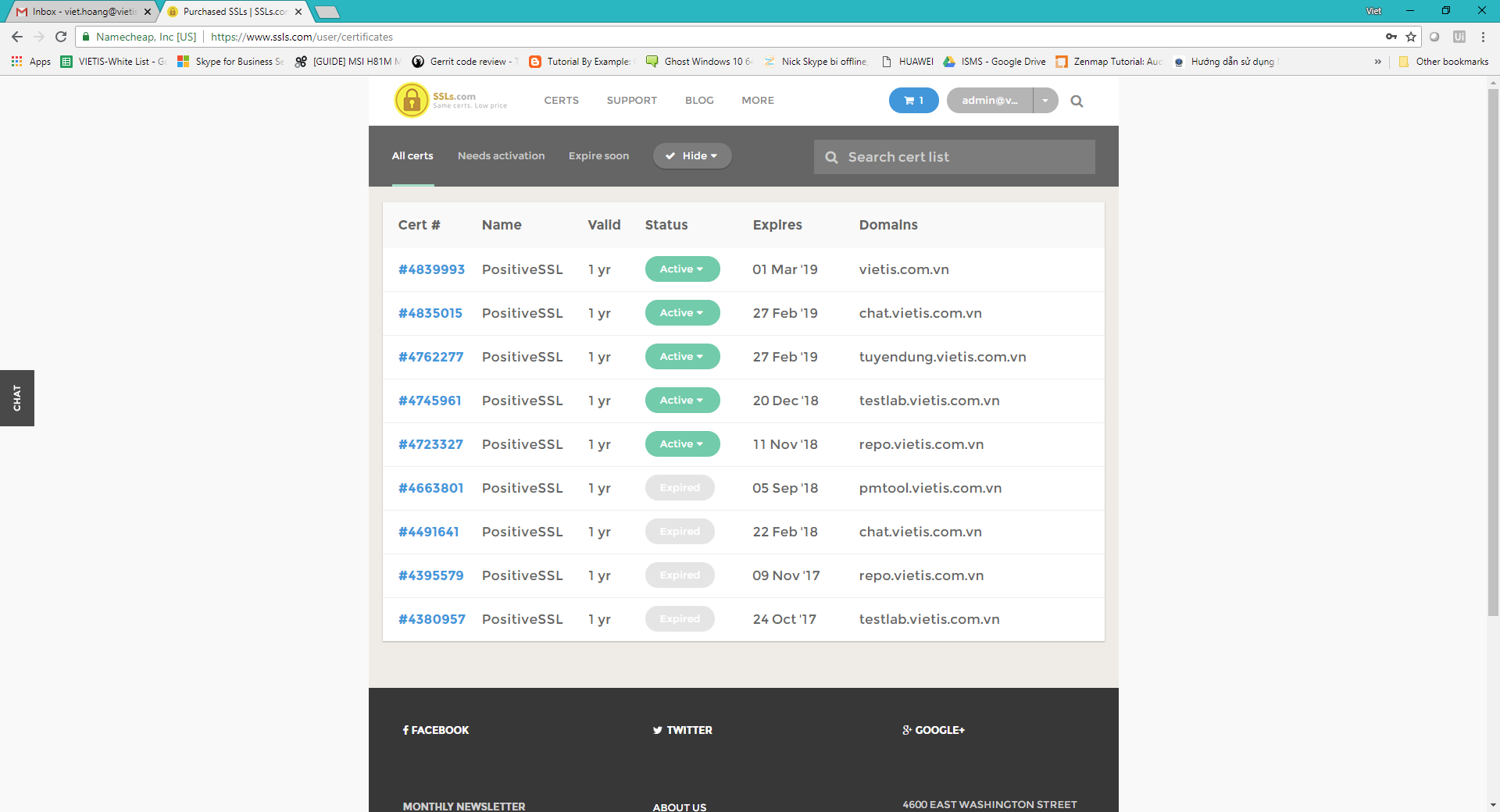
User/Pass: [admin@vietis.com.vn](mailto:admin@vietis.com.vn) / vit@is@875

**2/ Kiểm tra tình trạng SSL:**

Sau khi đăng nhập, chọn Dropdown List ở chỗ username, bấm Purchased Certs, nhìn cái nào gần expire thì phải gia hạn.

Trường hợp bị expire như [pmtool.vietis.com.vn](http://pmtool.vietis.com.vn/) thì mình phải Purchase New

Cái này anh nên check định kỳ hàng tháng hoặc tự đặt schedule reminder để quản lý :)



**3/ Mua mới certificate:**

Bấm vào Certs trên TOP menu bar, sau đó chọn 1 loại, thường em chọn loại rẻ nhất là Possitive SSL với giá chỉ 9$/năm.  
(<https://www.ssls.com/ssl-certificates/comodo-positivessl>)

Trường hợp mua Wildcat cho tất cả \*.[vietis.com.vn](http://vietis.com.vn/) thì mắc hơn (94$/yr),

nhưng anh có thể đề xuất nếu tổng chi phí Possitive SSL  cao hơn Wildcat.

**4/ Cài đặt:**

Trong [ssls.com](http://ssls.com/) có hướng dẫn đầy đủ, chi tiết các bước rồi, nên em ko nhắc lại nữa. Anh chỉ cần lưu ý mấy điểm sau

a) Chọn đúng loại Cert cho dòng Window Server hoặc Linux Server (chọn nhầm thì lại phải dùng tool convert Cert từ loại này sang loại kia)

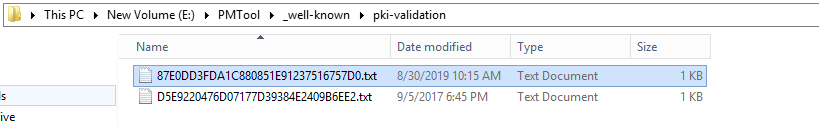
b) Xác thực domain: Có 2 cách

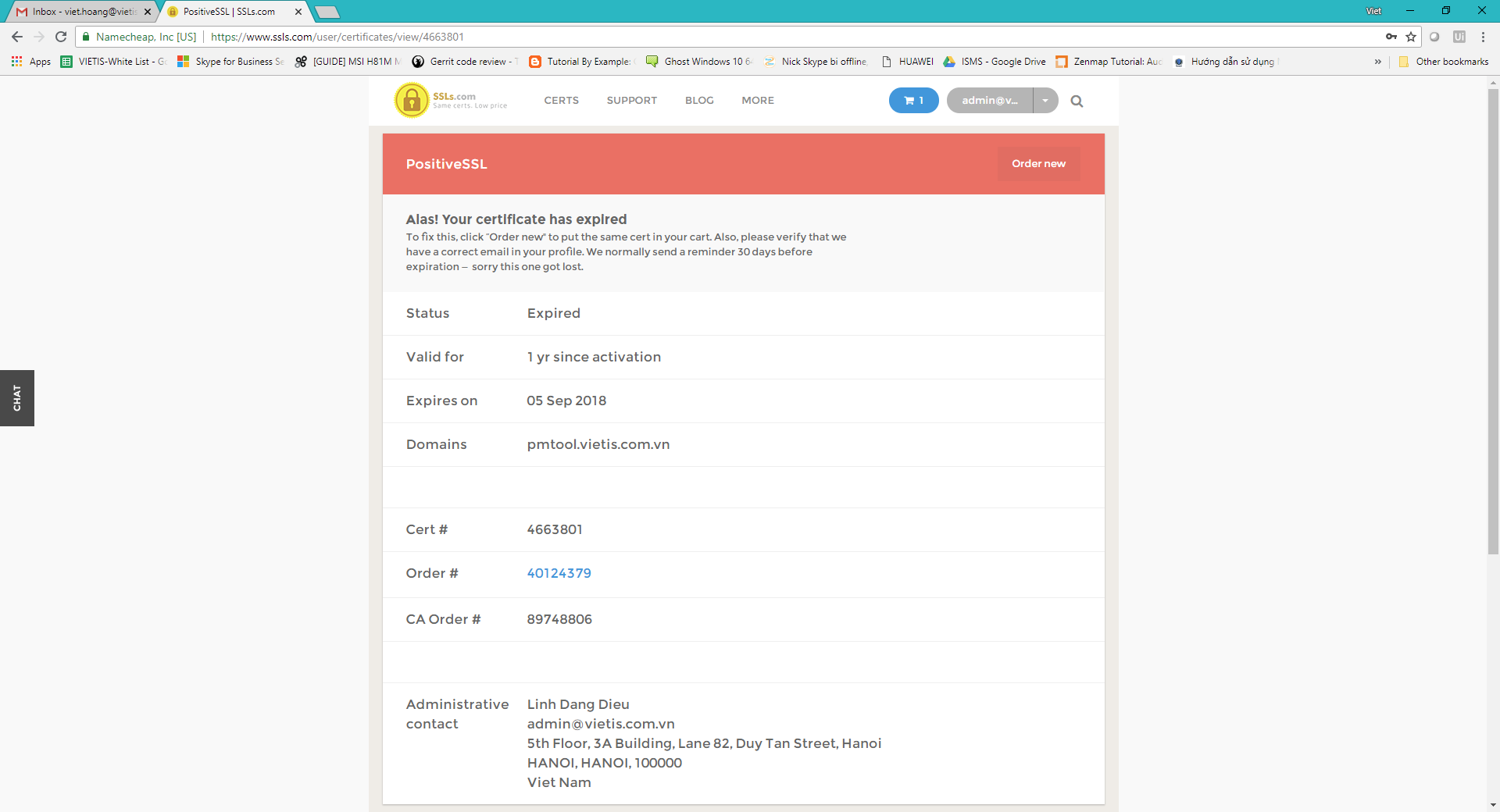
   + Bằng địa chỉ email [admin@vietis.com.vn](mailto:admin@vietis.com.vn), cái này anh ping em để FW lại mail từ admin về cho anh.

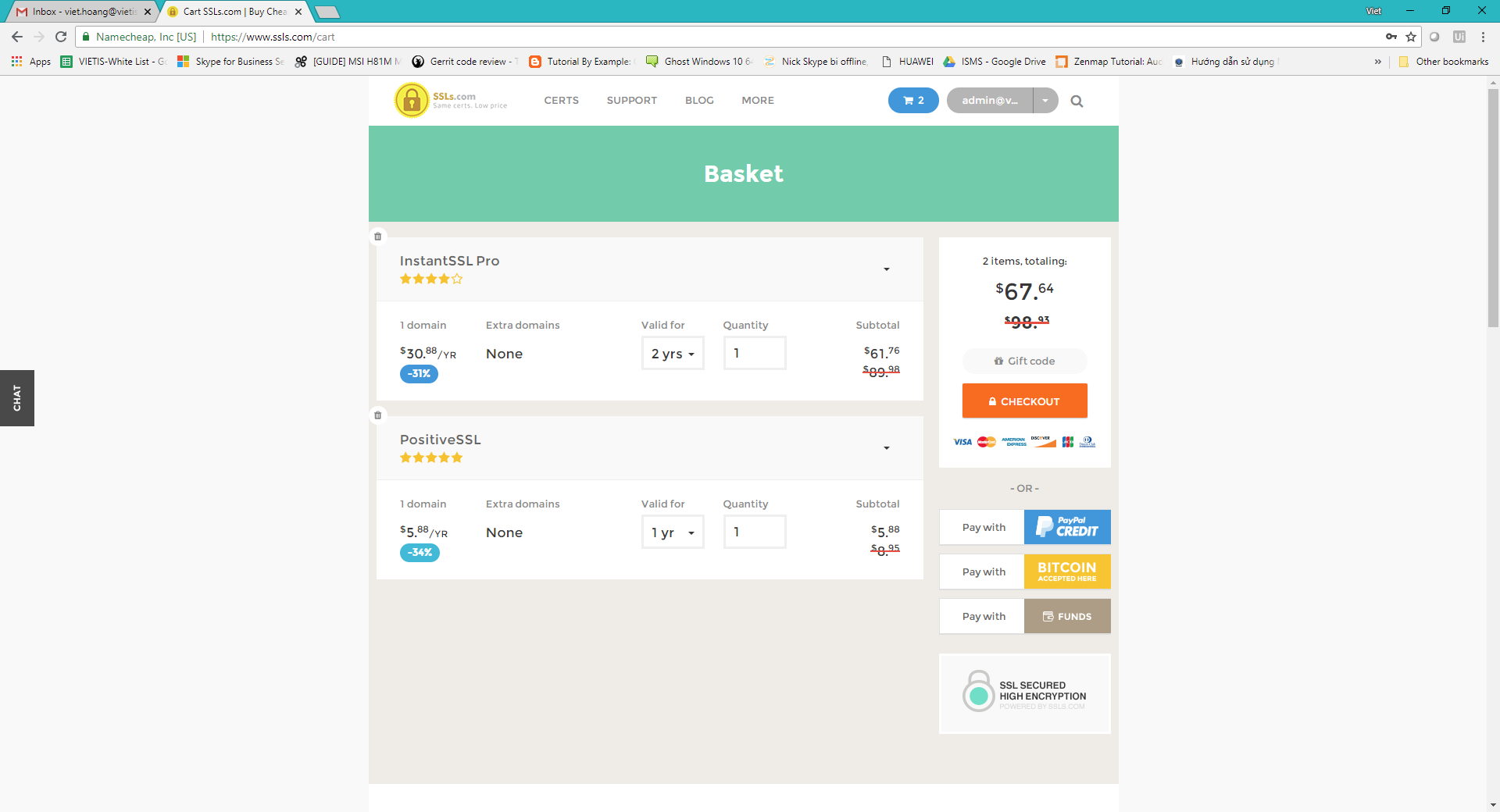
   + Bằng cách đặt 1 file txt vào root folder của tên miền để nó tự query vào và xác thực (cái này ko khả thi vì mình hay dùng Port, nó ko chấp nhận)

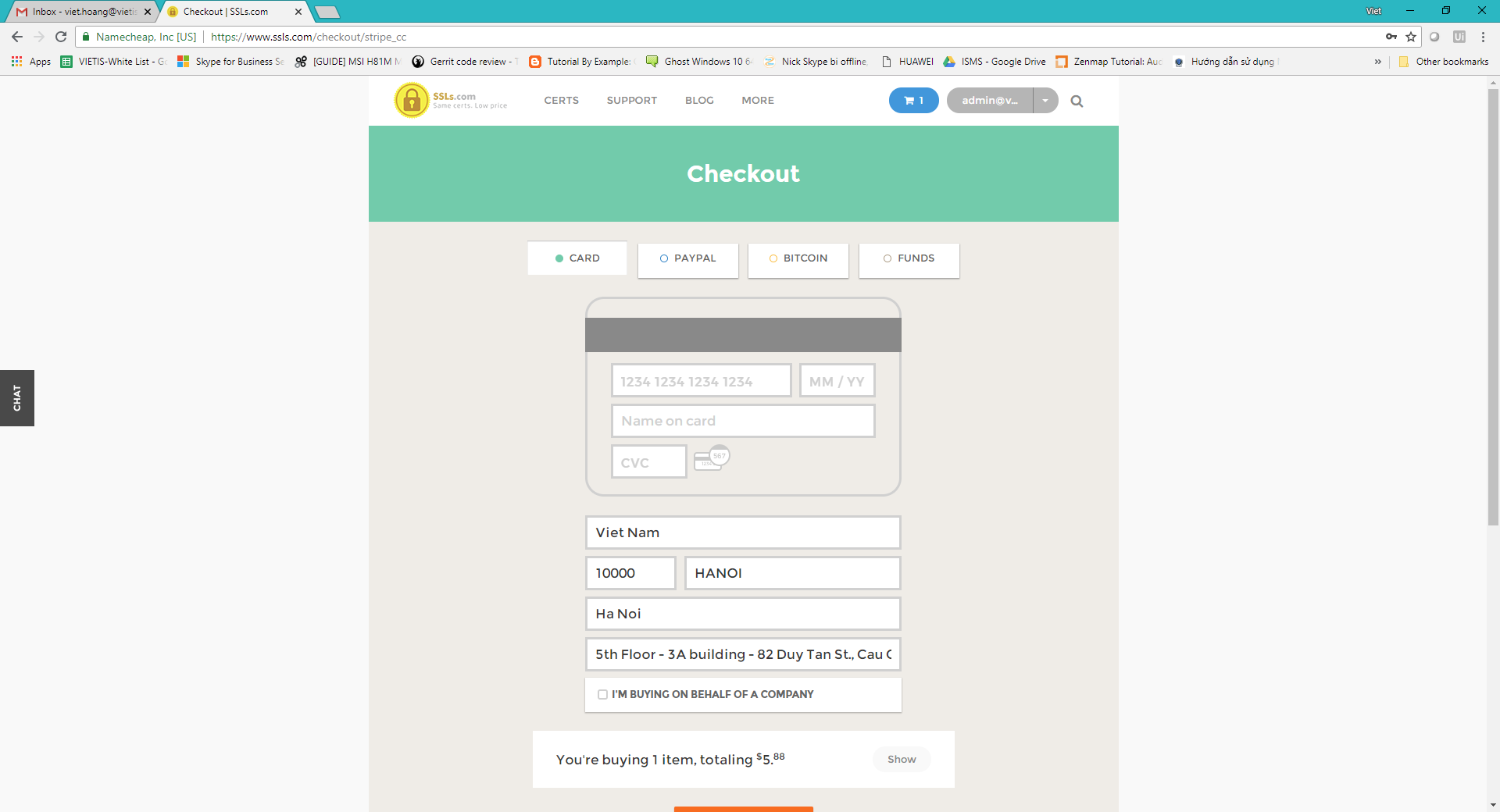
*VD: nó sẽ xác thực tên miền*[*pmtool.vietis.com.vn*](http://pmtool.vietis.com.vn/)*là của mình bằng việc truy xuất qua URL ngoài bằng*[*http://pmtool.vietis.com.vn/file-validate.txt*](http://pmtool.vietis.com.vn/file-validate.txt)

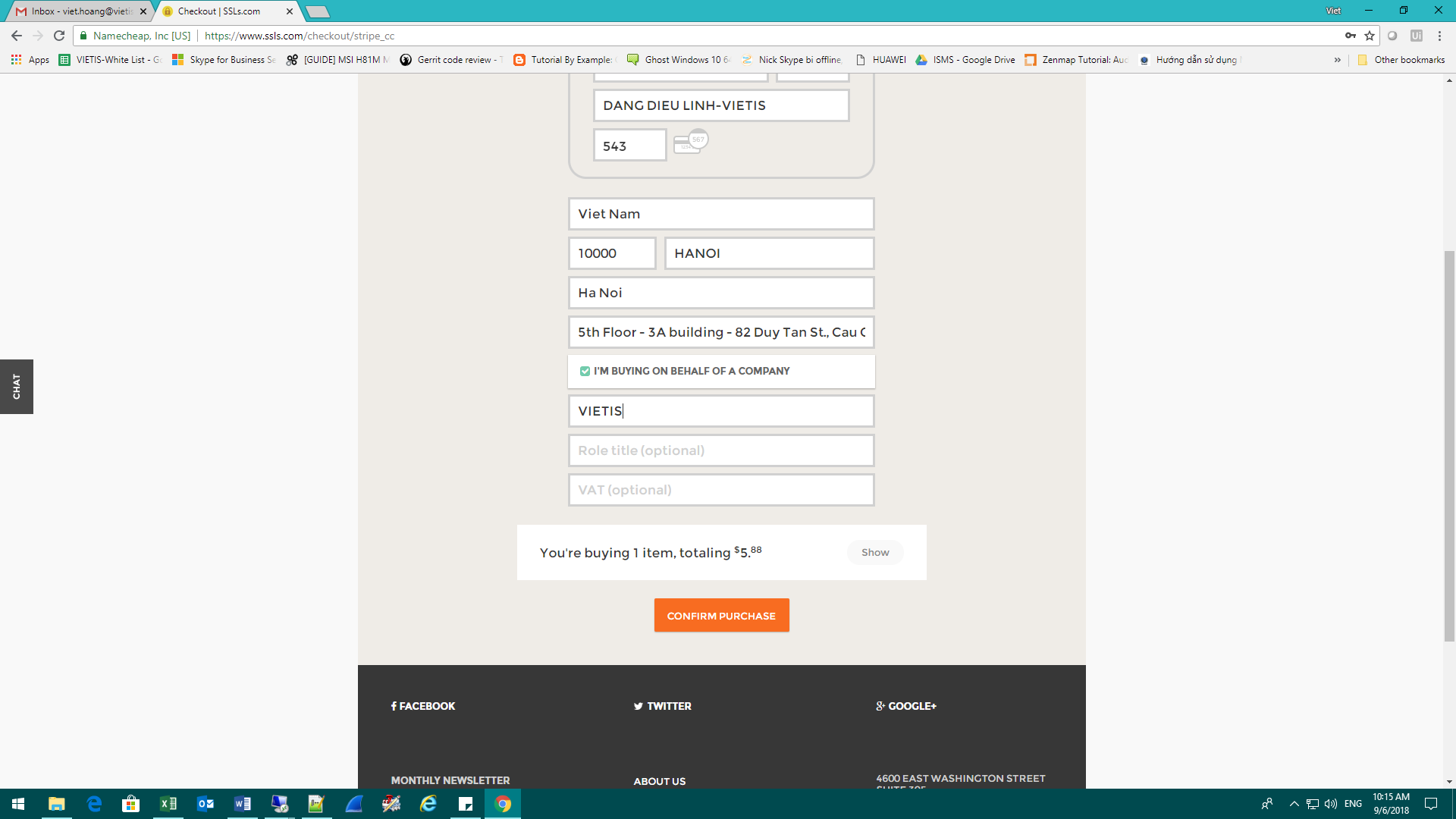
*file-validate chính là file nó gửi cho mình và bảo mình copy lên.*

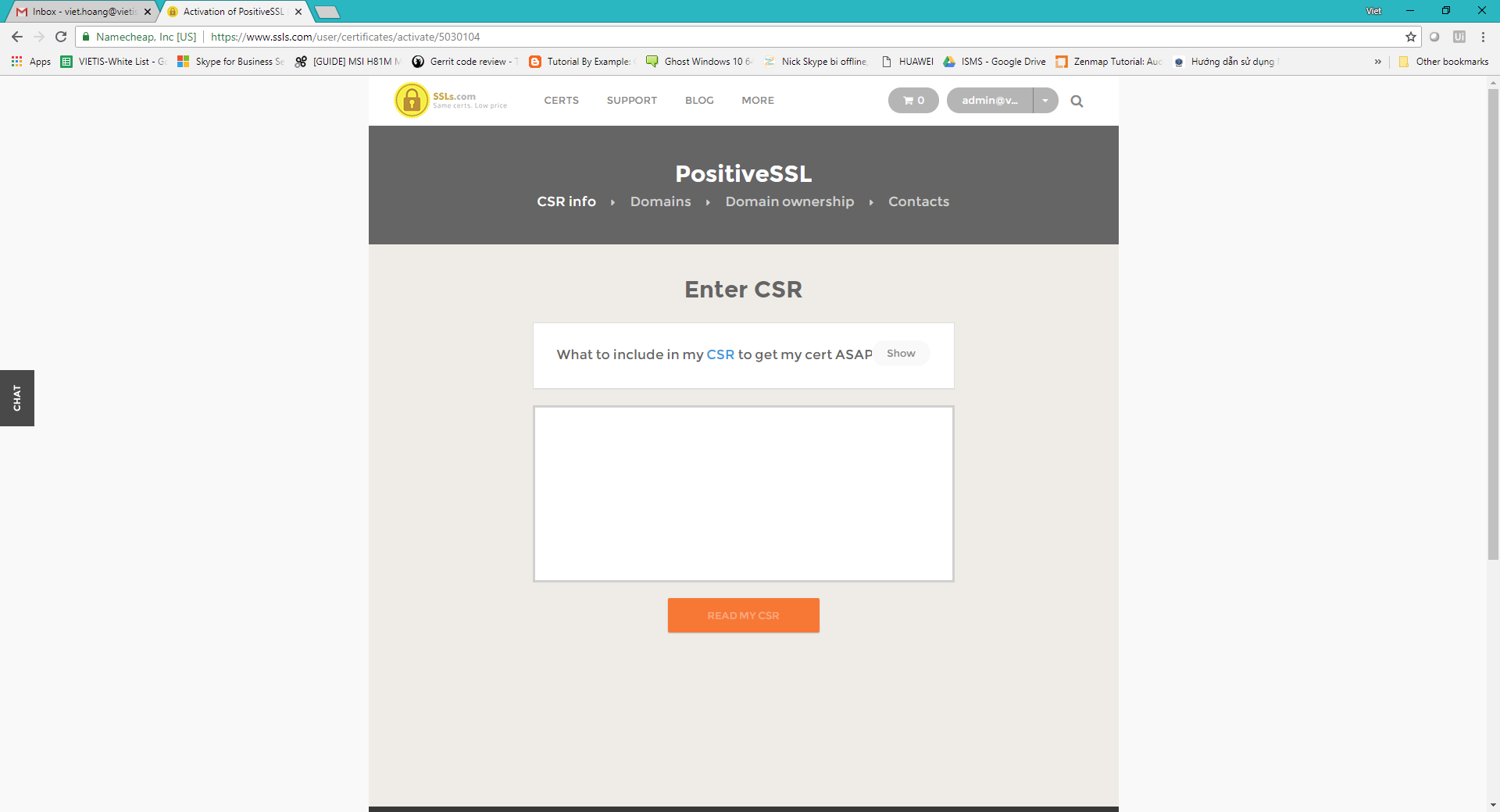


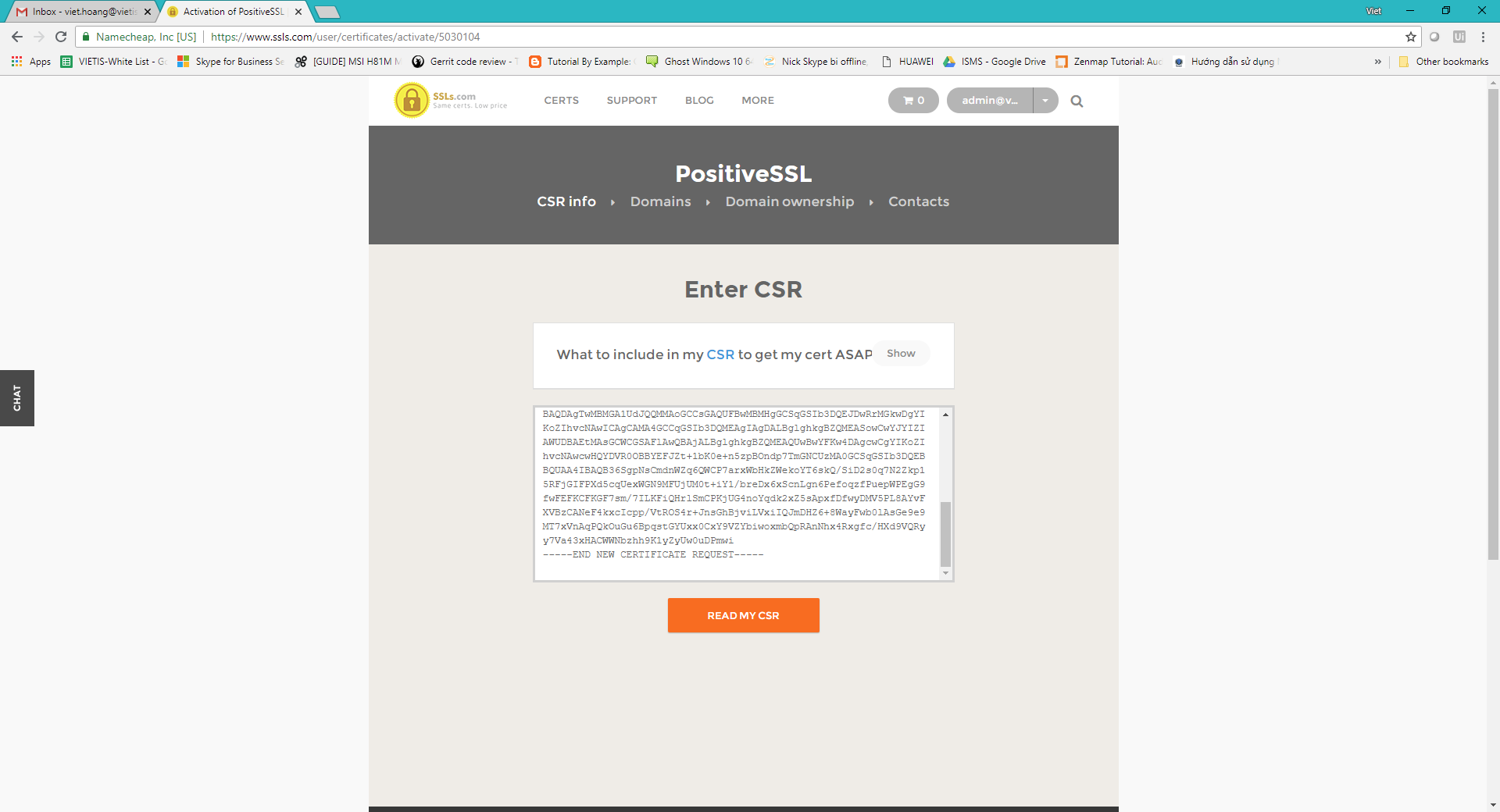


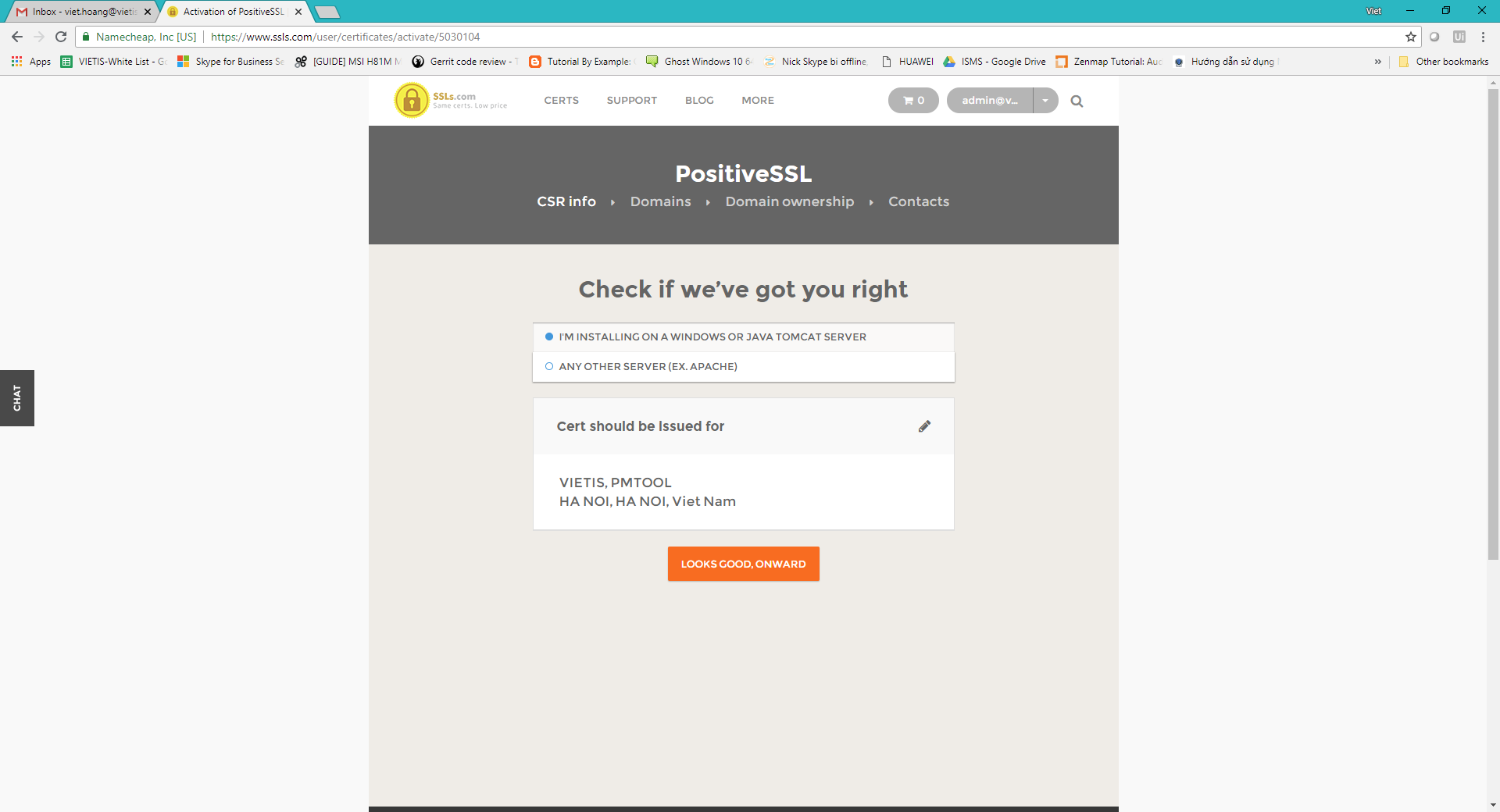


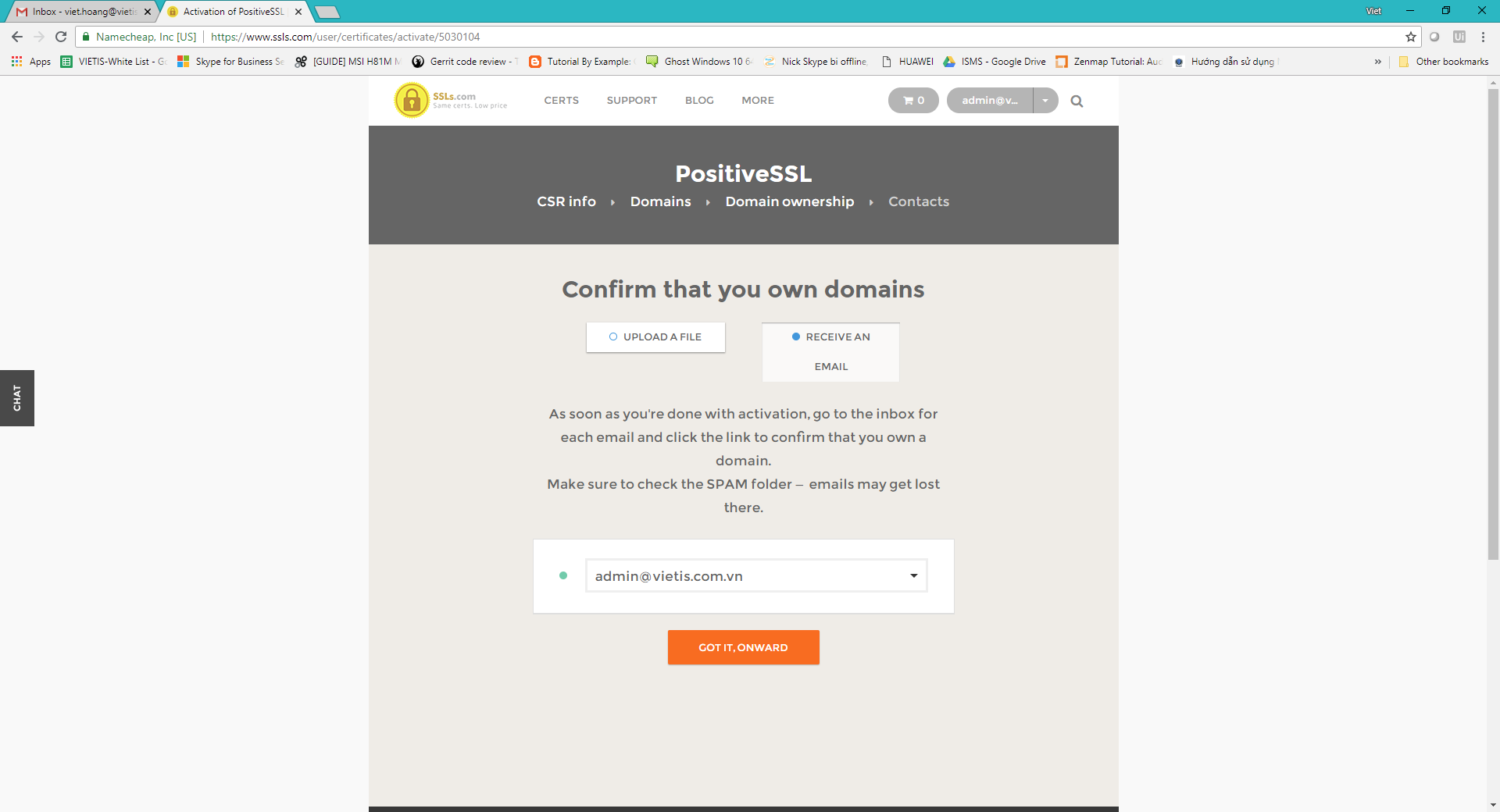


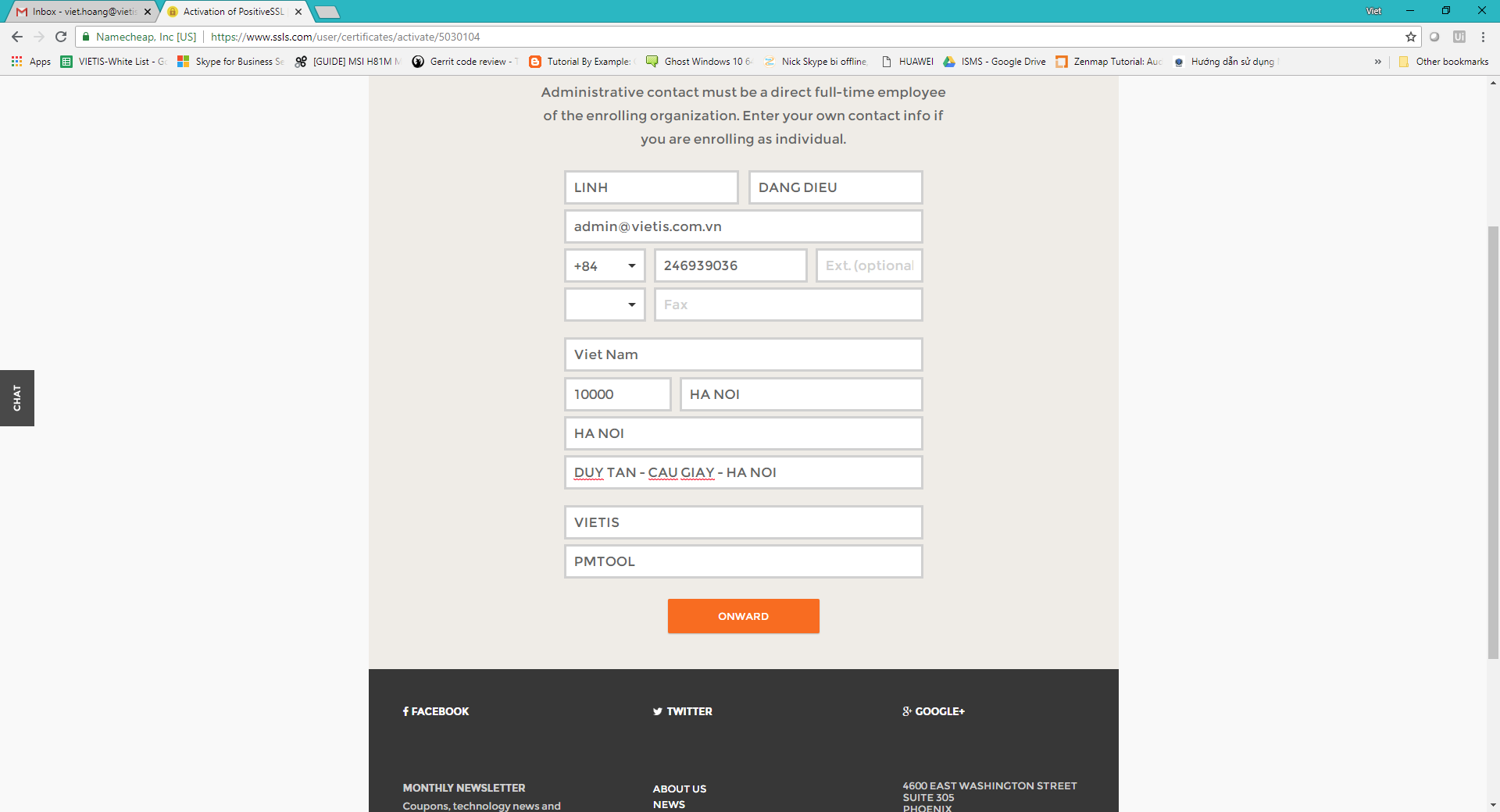


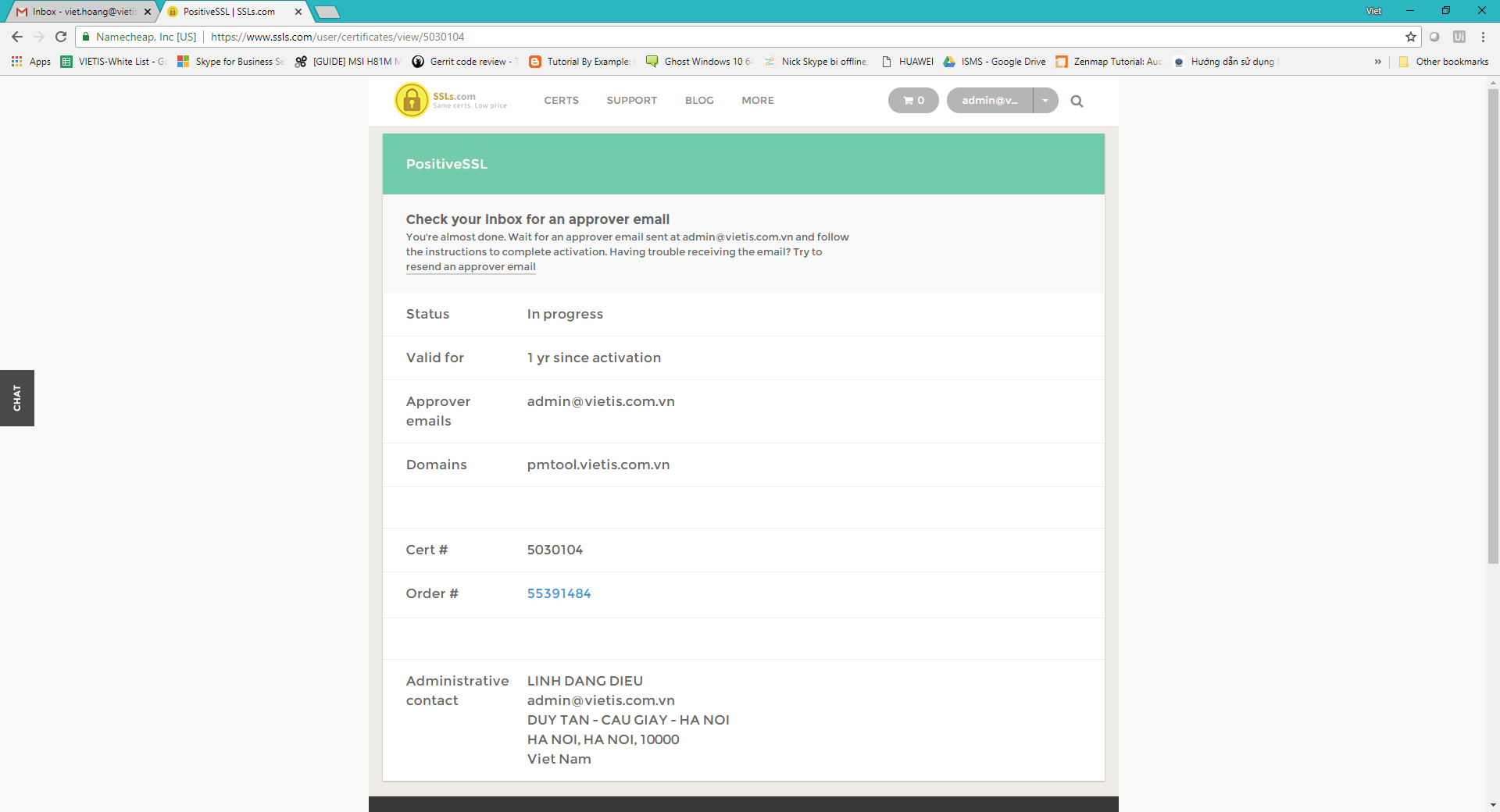


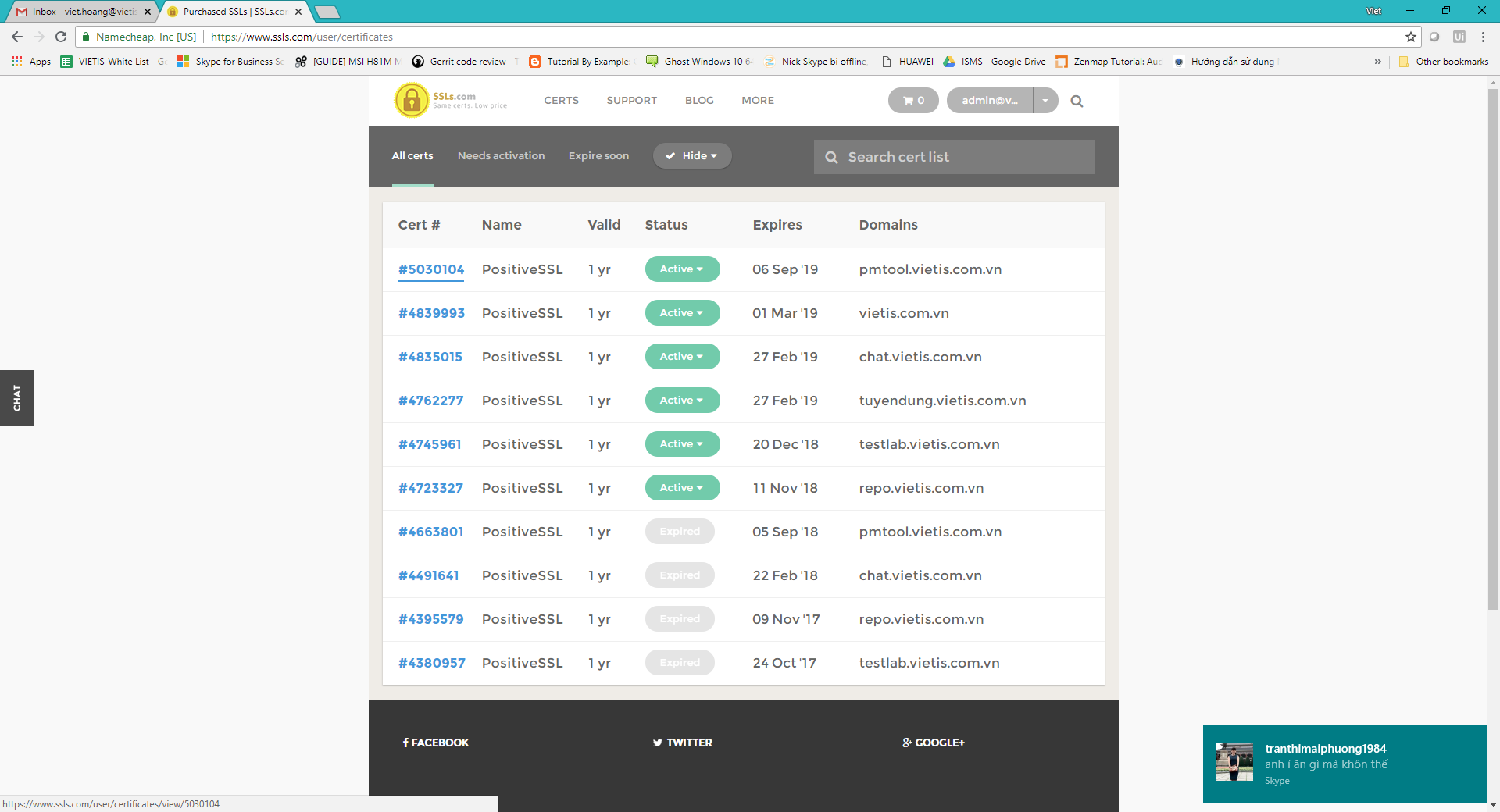












Đợi confirm từ email Admin@

Download file về

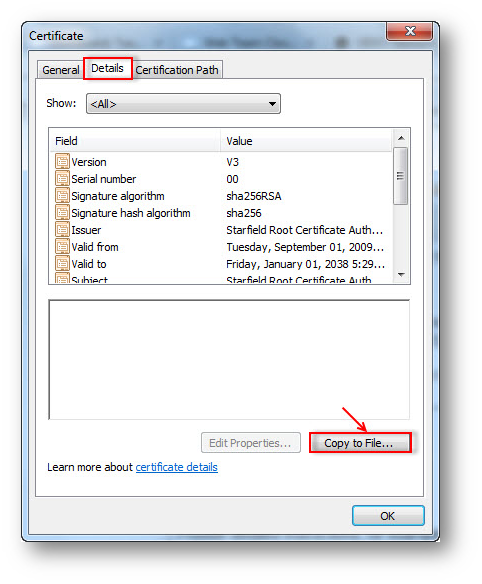
Giải nén

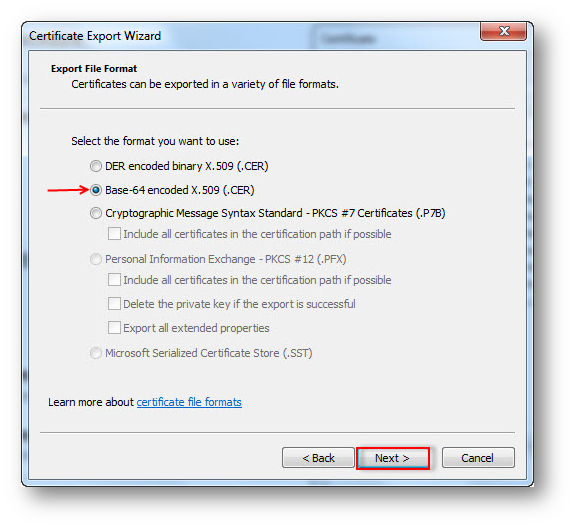
Double-click on the \*.crt file to open it into the certificate display.

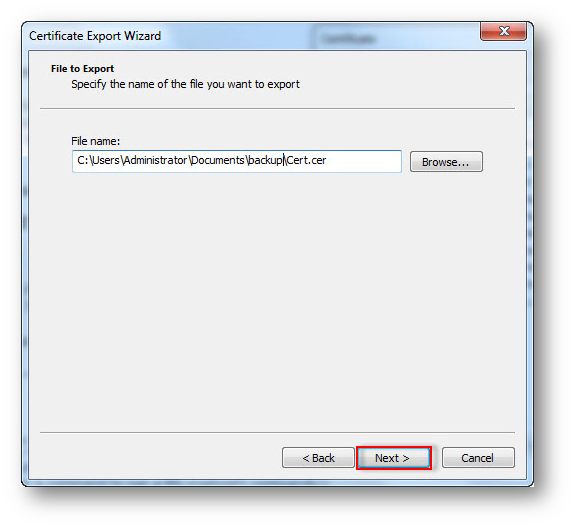
1. Select the **Details** tab, then select the **Copy to file** option.

export từ crt -> cer.

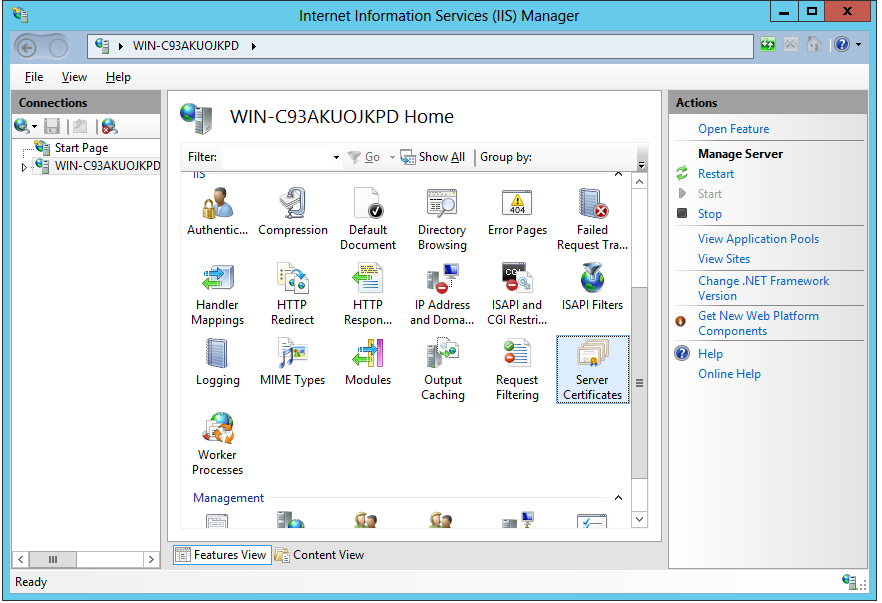
https://www.sonicwall.com/support/knowledge-base/how-to-convert-a-certificate-file-from-crt-to-cer/170504597576961/

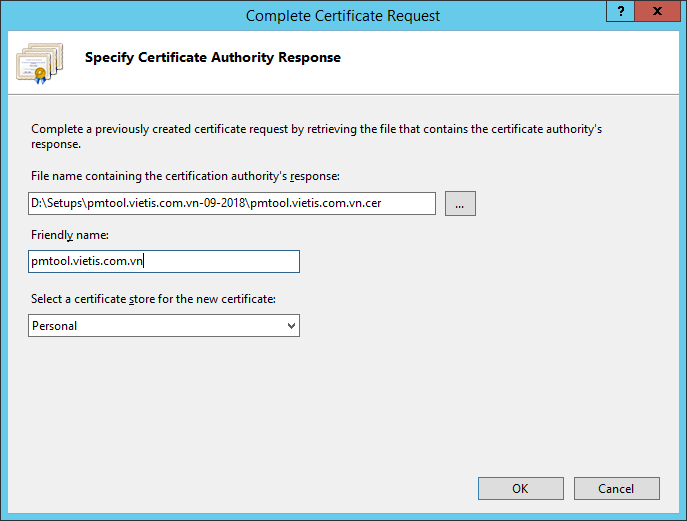




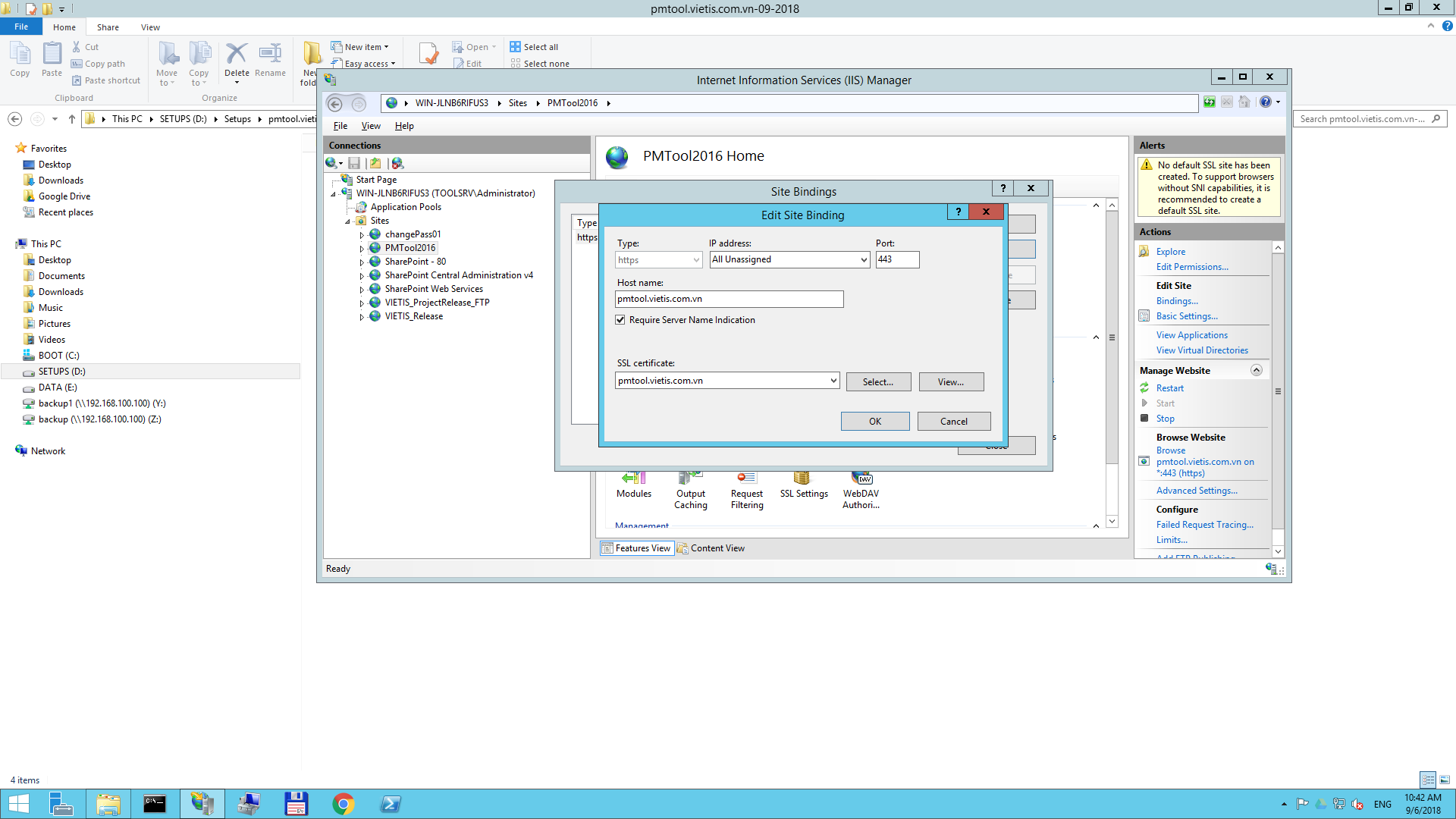


Complete cer





Binding SSL cho PMTOOL và CALLOG



<https://www.digicert.com/csr-ssl-installation/iis-8-and-8.5.htm>

<https://www.sonicwall.com/en-us/support/knowledge-base/170504597576961>

openssl genrsa -out tecadmin.net.key 2048

openssl req -new -key tecadmin.net.key -out tecadmin.net.csr

openssl genrsa -out ~/domain.com.ssl/domain.com.key 2048

openssl req -new -sha256 -key ~/domain.com.ssl/domain.com.key -out ~/domain.com.ssl/domain.com.csr

$ openssl req -new -key privkey.pem -out cert.csr -newkey rsa:2048

openssl req -nodes -newkey rsa:2048 repo.vietis.com.vn.key -out repo.vietis.com.vn.csr

openssl req -new -key repo.vietis.com.vn.key -out 20171107repo.vietis.com.vn.csr

openssl req -nodes -new -key repo.vietis.com.vn.key -out 20171107repo.vietis.com.vn.csr

https://gist.github.com/bradmontgomery/6487319#install-the-commodo-ssl-cert

cat STAR\_example\_com.crt STAR\_example\_com.ca-bundle > ssl-bundle.crt

https://gist.github.com/bradmontgomery/6487319

https://www.entrust.com/open-ssl-csr-generator/

nginx['ssl\_certificate'] = "/etc/gitlab/ssl/ssl-bundle.crt"

nginx['ssl\_certificate\_key'] = "/etc/gitlab/ssl/repo.vietis.com.vn.key"

Step 1: tao key moi

openssl req -new -newkey rsa:2048 -nodes -keyout example\_com.key -out example\_com.csr

==> repo.vietis.com.vn.key

==> repo.vietis.com.vn.crt

openssl req -new -newkey rsa:2048 -nodes -out repo.vietis.com.vn.scr -keyout repo.vietis.com.vn.key -subj "/C=VN/ST=084/L=024/O=VIETIS/OU=VIETIS JSC/CN=repo.vietis.com.vn"

Step 2: gui cho ben ban CER

Open File CER -> COPY Content -> Paste to SSL site

BB

/var/www/tuyendungvietis.dev/.well-known/pki-validation

312042C556957B9FCB973C5F83C0F84C.txt

**Step 3**: get back tu cer 3 file:

repo.vietis.com.vn.ca-bundle

repo.vietis.com.vn.crt

repo.vietis.com.vn.p7b

Step 4:

cat repo.vietis.com.vn.crt repo.vietis.com.vn.ca-bundle > ssl-bundle.crt

Step 5: copy vao /git/ssl

ssl-bundle.crt

repo.vietis.com.vn.key

openssl req -new -newkey rsa:2048 -nodes -out repo.vietis.com.vn.scr -keyout repo.vietis.com.vn.key -subj "/C=VN/ST=084/L=024/O=VIETIS/OU=VIETIS Software Corporation/CN=repo.vietis.com.vn"

=======================

Update thong tin email

Account: auto@vietis.com.vn,

vis@auto@00000

pmtool@vietis.com.vn

Password: vis@pmt@345

vi /etc/gitlab/gitlab.rb

gitlab\_rails['smtp\_password'] = "vis@pmt@1234"

mattermost['email\_smtp\_password'] = "vis@pmt@345"

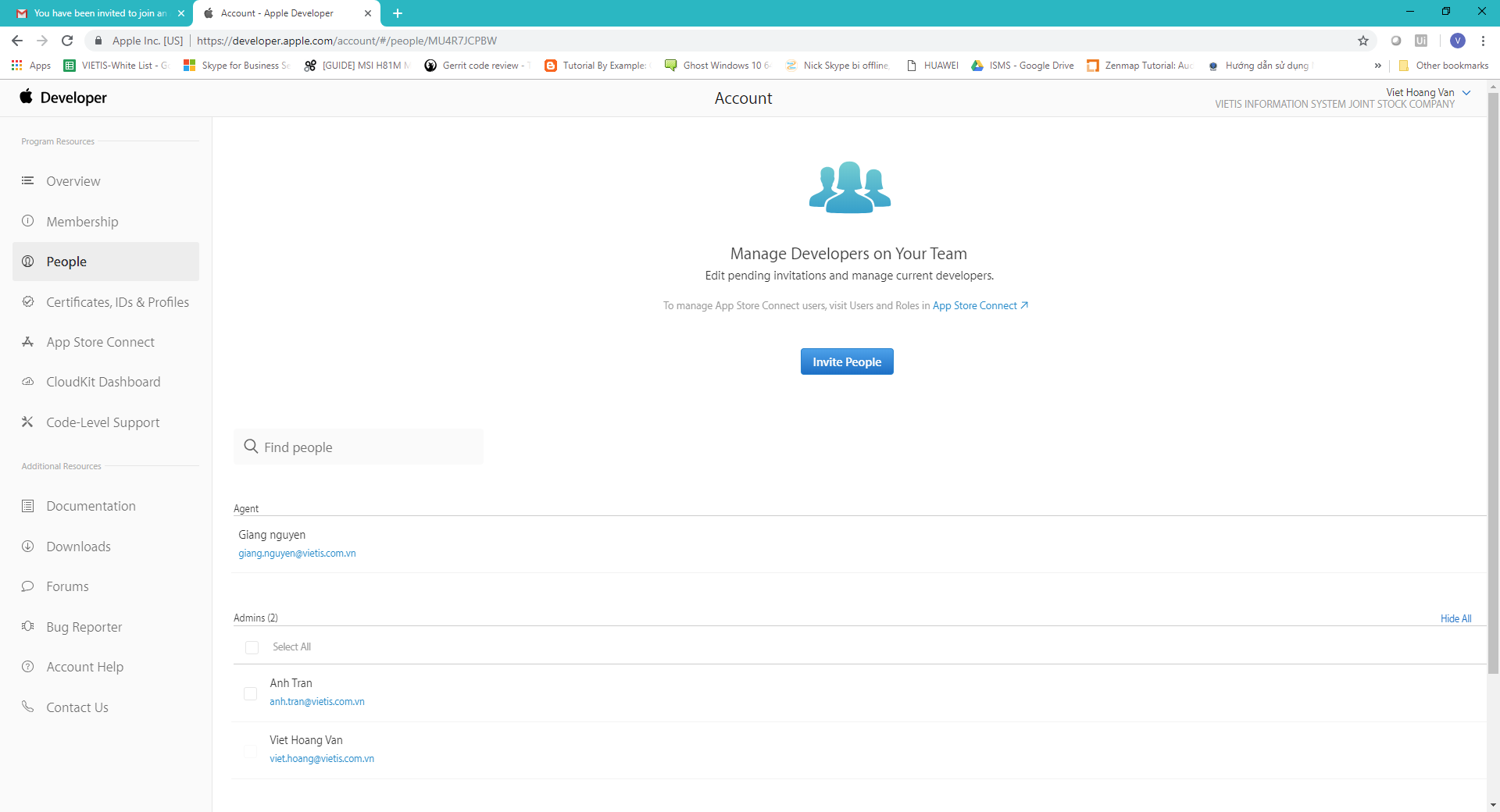
gitlab-ctl reconfigure

openssl req -new -newkey rsa:2048 -nodes -out repo.vietis.com.vn.scr -keyout repo.vietis.com.vn.key -subj "/C=VN/ST=084/L=024/O=VIETIS/OU=VIETIS Software Corporation/CN=repo.vietis.com.vn"

3 tháng 1 lần, vào các ngày 1/2, 1/5, 1/8, 1/11 hệ thống mail sẽ tự động bị reset ==> Anh update lại password nhé.

<https://www.ssls.com/user/certificates>

Tháng 10 expire repo



Invite people theo email @vietis.com.vn

as members

CHAT:

openssl req -new -newkey rsa:2048 -nodes -out chat.vietis.com.vn.csr -keyout chat.vietis.com.vn.key -subj "/C=VN/ST=084/L=024/O=VIETIS/OU=VIETIS Software Corporation /CN=chat.vietis.com.vn"

openssl req -new -newkey rsa:2048 -nodes -out chat.vietis.com.vn.csr -keyout chat.vietis.com.vn.key -subj "/C=VN/ST=084/L=024/O=VIETIS/OU=VIETIS Software Corporation /CN=chat.vietis.com.vn"

cat chat\_vietis\_com\_vn.crt chat\_vietis\_com\_vn.ca-bundle > ssl-bundled.crt

WWW

OLD: openssl req -new -sha256 -key vietis.com.vn.key -out tuyendung.vietis.com.vn.csr

openssl req -new -newkey rsa:2048 -nodes -out tuyendung.vietis.com.vn.csr -keyout tuyendung.vietis.com.vn.key -subj "/C=VN/ST=084/L=024/O=VIETIS/OU=VIETIS Software Corporation /CN=tuyendung.vietis.com.vn"

openssl req -new -newkey rsa:2048 -nodes -out www.vietis.com.vn.scr -keyout www.vietis.com.vn.key -subj "/C=VN/ST=084/L=024/O=VIETIS/OU=VIETIS Software Corporation/CN=vietis.com.vn"

SSLCertificateFile /etc/pki/tls/certs/vietis.com.vn/vietis\_com\_vn.crt

SSLCertificateKeyFile /etc/pki/tls/certs/vietis.com.vn/vietis.com.vn.key

SSLCertificateFile /etc/pki/tls/certs/tuyendung.vietis.com.vn/tuyendung\_vietis\_com\_vn.crt

SSLCertificateKeyFile /etc/pki/tls/certs/tuyendung.vietis.com.vn/tuyendung.vietis.com.vn.key

ssl\_certificate /opt/cert/ssl-bundled.crt;

ssl\_certificate\_key /opt/key/chat.vietis.com.vn.key;

/opt/key/chat.vietis.com.vn.key

/opt/cert/ssl-bundled.crt

**Check a certificate**

Check a certificate and return information about it (signing authority, expiration date, etc.):

openssl x509 -in server.crt -text -noout

**Check a key**

Check the SSL key and verify the consistency:

openssl rsa -in server.key -check

**Check a CSR**

Verify the CSR and print CSR data filled in when generating the CSR:

openssl req -text -noout -verify -in server.csr

**Verify a certificate and key matches**

These two commands print out md5 checksums of the certificate and key; the checksums can be compared to verify that the certificate and key match.

openssl x509 -noout -modulus -in server.crt| openssl md5  
openssl rsa -noout -modulus -in server.key| openssl md5

**openssl x509 -noout -modulus -in** chat.vietis.com.vn**.crt | openssl md5**

**openssl rsa -noout -modulus -in** chat.vietis.com.vn.key **| openssl md5**

**2020**

Step 1: tao key moi

openssl req -new -newkey rsa:2048 -nodes -out vietis.com.vn.csr -keyout vietis.com.vn.key -subj "/C=VN/ST=084/L=024/O=VIETIS/OU=VIETIS JSC/CN=vietis.com.vn"

openssl req -new -newkey rsa:2048 -nodes -out tuyendung.vietis.com.vn.csr -keyout tuyendung.vietis.com.vn.key -subj "/C=VN/ST=084/L=024/O=VIETIS/OU=VIETIS JSC/CN=tuyendung.vietis.com.vn"

openssl req -new -newkey rsa:2048 -nodes -out chat.vietis.com.vn.csr -keyout chat.vietis.com.vn.key -subj "/C=VN/ST=084/L=024/O=VIETIS/OU=VIETIS JSC/CN=chat.vietis.com.vn"

Step 2: gui cho ben ban CER

Open File CER -> COPY Content -> Paste to SSL site

**Step 3**: get back tu cer 3 file:

repo.vietis.com.vn.ca-bundle

repo.vietis.com.vn.crt

repo.vietis.com.vn.p7b

Step 4:

cat repo.vietis.com.vn.crt **repo.vietis.com.vn.ca-bundle** > ssl-bundle.crt

Step 5: copy vao /git/ssl

ssl-bundle.crt

repo.vietis.com.vn.key

chú ý chat:

ssl\_certificate /opt/cert/ssl-bundled.crt;

ssl\_certificate\_key /opt/key/chat.vietis.com.vn.key;

openssl req -new -newkey rsa:2048 -nodes -out vietis.jp.csr -keyout vietis.jp.key -subj "/C=JP/ST=29/L=Gotanda/O=VIETIS/OU=VIETIS Solution/CN=vietis.jp"

Step 2: gui cho ben ban CER

Open File CER -> COPY Content -> Paste to SSL site

**Step 3**: get back tu cer 3 file like this:

vietis\_jp.crt

vietis\_jp.ca-bundle

Step 4:

cat vietis\_jp.crt vietis\_jp.ca-bundle > ssl-bundle.crt (hhoặc tên gì tùy)

Step 5: copy vao /git/ssl

ssl-bundle.crt

vietis.jp.key

Em có transfer cho đội dự án rồi a ạ.

Chỗ này ngoài setup apache như bên dưới.

SSLVerifyClient require

SSLVerifyDepth 10

- Cần setup thêm SSLCACertificateFile(certificate của CA) để apache validate được certificate của client.

- Ngoài ra do môi trường của khách hàng nên có setup thêm ajp để đưa request từ apache sang tomcat.

ProxyPass / ajp://127.0.0.1:8009/

ProxyPassReverse / ajp://127.0.0.1:8009/

***<VirtualHost [IP="ADDRESS"]:443  
...  
SSLCertificateFile /absolute/path/to/your\_domain\_name.crt  
SSLCertificateKeyFile /absolute/path/to/your\_domain\_name.key  
SSLCertificateChainFile /absolute/path/to/your\_domain\_name.ca\_bundle  
...  
</VirtualHost>***

* **SSLCertificateFile** directive shows the path to your domain’s certificate file.  
  Example: ***SSLCertificateFile /etc/httpd/conf/ssl/certificate.crt***
* **SSLCertificateKeyFile** leads to the Private Key file associated with your certificate file.  
  Example: ***SSLCertificateKeyFile /etc/httpd/conf/key/private.key***
* **SSLCertificateChainFile** directive shows the location of the CA Bundle or Certificate Authority Chain file.  
  Example: ***SSLCertificateChainFile /etc/httpd/conf/ssl/bundle.crt***

# How to move an SSL Certificate from one Server to Another

<https://www.namecheap.com/support/knowledgebase/article.aspx/9636/69/how-to-move-a-certificate-between-apache-web-servers/>

<https://www.eurovps.com/faq/how-to-move-an-ssl-certificate-from-one-server-to-another/>

<https://kb.pavietnam.vn/huong-dan-cach-chuyen-chung-chi-ssl-giua-cac-may-chu-windows.html>

<https://manage.accuwebhosting.com/knowledgebase/1240/How-to-export-an-SSL-certificate-from-Apache-server.html>

Mình có 3 file

domain.key

domain.crt

domain.ca

Sau đó chạy lệnh sau để Convert

openssl pkcs12 -export -out vinawebsite.pfx -inkey domain.key -in domain.crt -certfile domain.ca

* *out certificate.pfx*: Tên file pfx sau khi export
* *key*: Tên file private key
* *crt*: Tên file CRT

Sau khi Convert thành công bạn sẽ thấy có 1 file .pfx tại thư mục đó

Open the command terminal in Linux server and execute the below command to convert the .pfx certificate to the .crt and private key format.

openssl pkcs12 -in eurovps.pfx -out testconvert.txt –nodes

openssl pkcs12 -export -out eurovpstest.pfx -inkey private.key -in primary.crt -certfile intermediate.crt

The converted .txt file will have two parts, the private key section and the certificate section.

Copy the text included in —–BEGIN PRIVATE KEY—– to —–END PRIVATE KEY—– to another file and name it as the domain.key file.

Copy the text included in —–BEGIN CERTIFICATE—– to —–END CERTIFICATE—– to another file and name it as domain.crt.

SSLEngine on

SSLCertificateFile /etc/ssl/crt/primary.crt

SSLCertificateKeyFile /etc/ssl/crt/private.key

SSLCertificateChainFile /etc/ssl/crt/intermediate.crt