

## Ressource Prof : Certificats

### VM prof pour l'autorité de certification (CA)

#### Présentation

La VM 'debianProflot' est livrée avec ce TP. Cette fiche présente les manipulations faites sur la VM **debianProflot** pour vous permettre de refaire votre propre VM à l'identique ou adapter votre VM existante. La VM a un serveur FTP configuré pour que le compte «etudiant » (mot de passe 'etudiant') upload et télécharge sur son home directory. Vous pouvez aussi choisir un autre système pour l'échange de fichiers (demande de certificats .csr et certificats .crt).

La fiche reprend également toutes les étapes nécessaires à la création des clefs / certificats.

#### Infos sur la VM debianProflot

- Compte `prof` (sudo) / mot de passe '`prof`' (il est conseillé de changer le mot de passe qui peut être facilement essayé par des étudiants),
- Compte `etudiant` (compte simple) / mot de passe '`etudiant`' ,
- Le user '`prof`' est ajouté au groupe '`etudiant`' ,
- Packages `mosquitto` et `mosquitto-clients` et `tcpdump` installés,
- Serveur FTP `vsftpd` installé et configuré pour que l'utilisateur '`etudiant`' puisse uploader / télécharger des fichiers (pour les .csr et .crt) (utilisateur '`prof`' appartient au groupe '`etudiant`' et peut lire / écrire dans le home directory '`etudiant`'),
- Les fichiers utilisés pour le TLS sont dans le home directory de '`prof`' et copiés dans les répertoires de configuration des logiciels.

#### Configuration du broker mosquitto

Le service est automatiquement lancé au boot du système avec le fichier de configuration `/etc/mosquitto/conf.d/tp.conf` configuré pour des connexions anonymes, sans mot de passe pour du local.

Deux fichiers de configuration sont par ailleurs disponibles dans `/home/prof`

- `mosquitto-tls.conf` : pour le broker sécurisé
- `mosquitto.conf` : pour le broker non sécurisé

Démarrage manuel pour choisir la configuration :

```
/usr/sbin/mosquitto -c <mosquito.conf> -d
```

## Procédures pour créer une VM ou modifier une VM existante

En plus du compte prof (sudo) : installer les packages mosquito, mosquito-clients, vsftpd et tcpdump.

Création du compte 'etudiant' (mot de passe suggéré 'etudiant'), ajout de 'prof' au groupe 'etudiant'.

Modifier le profil de l'utilisateur 'etudiant' pour modifier les droits par défaut des fichiers et dossiers créés (pour donner droits au groupe 'etudiant')

→ ajouter la ligne ci-dessous au fichier `.bashrc`  
`umask 002`

Configuration de VSFTPD pour que 'etudiant' puisse uploader / télécharger ses fichiers (pour l'échange des fichiers .csr / .crt).

Lignes modifiées de /etc/vsftpd.conf :

```
# Uncomment this to allow local users to log in.
local_enable=YES

# Uncomment this to enable any form of FTP write command.
write_enable=YES

# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
local_umask=002
```

Redémarre VSFTPD

```
sudo service vsftpd restart
```

## Utilitaire openssl

Openssl est installé en natif avec Debian.

## Etapes à réaliser

Autorité de certification (CA Certificate Authority) (déjà fait sur la VM debianProfIot)

Etape	Commande	remarques
Création de la clef sur la VM Prof (entrer un mot de passe pour protéger la clef)	<code>prof@debianProfIot:~\$ openssl genrsa -des3 -out ca.key 2048</code> Enter PEM pass phrase: Verifying - Enter PEM pass phrase:	Une clef est créée dans le fichier <code>ca.key</code> spécifié avec l'option -out Mot de passe : 'prof' Donnée sensible (privée)
Créer un certificat X509 pour la CA signé avec cette clef	<code>prof@debianProfIot:~\$ openssl req -new -x509 -days 1826 -key ca.key -out ca.crt</code> Enter pass phrase for ca.key: <code>&lt;mot de passe pour la clef créée ci-dessus&gt;</code> 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]: <code>FR</code> State or Province Name (full name) [Some-State]: <code>France</code> Locality Name (eg, city) []: Organization Name (eg, company) [Internet Widgits Pty Ltd]: <code>Lycee</code> Organizational Unit Name (eg, section) []: <code>BTS CIEL</code> Common Name (e.g. server FQDN or YOUR name) []: <code>debianProfIot</code> Email Address []:	Mot de passe choisi pour la clef <code>ca.key</code> : 'prof' En fluo, les réponses au script de création du certificat. <b>Ne pas mettre d'accents !</b> <b>En rouge : le nom doit correspondre au hostname</b> L'option -days indique le nombre de jours de validité du certificat.  Un certificat est créé dans le fichier <code>ca.crt</code> (option -out)
<p>A ce stade vous avez deux fichiers <code>ca.key</code> et <code>ca.crt</code></p> <p>La VM prof jouera le rôle d'autorité de certification (CA).</p>		

# Sciences et Techniques Industrielles

Portail national de ressources - éduscol

Création du certificat du broker de la VM Prof (les étudiants devront faire ces manipulations pour leurs propres brokers – voir TP)

Ces étapes sont déjà réalisées sur la VM debianProfIot.

Les étudiants enverront le fichier .csr par FTP à la CA, le prof génère les certificats .crt et les dépose dans /home/etudiant pour que l'étudiant puisse le récupérer.

Etape	Commande	remarques
Copier les fichiers SSL du broker	<code>prof@debianProfIot:~\$ openssl genrsa -out broker.key 2048</code>	Une clef est créée dans le fichier <code>broker.key</code> spécifié avec l'option -out Pas de mot de passe pour le broker Donnée sensible (privée)
Créer une demande de certificat X509	<code>prof@debianProfIot:~\$ openssl req -new -out broker.csr -key broker.key</code> 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]:FR State or Province Name (full name) [Some-State]:Occitanie Locality Name (eg, city) []: Organization Name (eg, company) [Internet Widgits Pty Ltd]:BTS CIEL Organizational Unit Name (eg, section) []: Common Name (e.g. server FQDN or YOUR name) []:debianProfIot Email Address []:  Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:prof An optional company name []:prof	En fluo, les réponses au script de création du certificat. Il ne faut pas mettre la même chose que pour la CA En rouge : le nom doit correspondre au hostname  Ne pas mettre d'accents !  Une demande de certificat est créée dans le fichier <code>broker.csr</code>
La CA fournit un certificat en signant le csr avec la clef ca.key	<code>prof@debianProfIot:~\$ openssl x509 -req -in broker.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out broker.crt -days 360</code> Certificate request self-signature ok subject=C = FR, ST = Occitanie, O = BTS CIEL, CN = debianProfIot Enter pass phrase for ca.key: <mot de passe pour la clef créée ci-dessus>	Le certificat est créé et signé par la CA et généré dans le fichier <code>broker.crt</code> Mot de passe de la clef : 'prof'
A ce stade vous avez trois nouveaux fichiers <code>broker.key</code> et <code>broker.csr</code> et <code>broker.crt</code> . le fichier <code>broker.csr</code> peut être supprimé.		

Configuration du borker mosquitto en mode sécurisé sur la VM prof (les étudiants devront faire ces manipulations pour leurs brokers)

Cette étape est déjà réalisée sur la VM debianProflot.

Etape	Commande	remarques
Copie des fichiers (clefs et certificats) dans les répertoires pour mosquitto	<p>On utilise les répertoires qui doivent déjà exister dans /etc/mosquitto</p> <pre>prof@debianProfIot:/etc/mosquitto\$ ls -l total 32 -rw-r--r-- 1 root root 230 9 juin 2021 aclfile.example drwxr-xr-x 2 root root 4096 19 déc. 19:11 ca_certificates drwxr-xr-x 2 root root 4096 19 déc. 19:11 certs drwxr-xr-x 2 root root 4096 22 déc. 10:47 conf.d -rw-r--r-- 1 root root 354 30 sept. 2023 mosquitto.conf -rw-r--r-- 1 root root 240 22 déc. 10:11 passwords -rw-r--r-- 1 root root 23 9 juin 2021 pskfile.example -rw-r--r-- 1 root root 355 9 juin 2021 pwfile.example prof@debianProfIot:/etc/mosquitto\$</pre> <p>copier le certificat du CA dans ca_certificates</p> <pre>\$ sudo cp /home/prof/ca.crt ca_certificates/</pre> <p>copier le certificat et la clef du broker dans le répertoire certs</p> <pre>\$ sudo cp /home/prof/broker.crt certs/ \$ sudo cp /home/prof/broker.key certs/</pre>	
Modifier la configuration du broker mosquitto	<pre># modification du port pour MQTTS listener 8883 protocol mqtt  # emplacement des fichiers copiés cafile /etc/mosquitto/ca_certificates/ca.crt keyfile /etc/mosquitto/certs/broker.key certfile /etc/mosquitto/certs/broker.crt # configuration du broker pour passage en SSL require_certificate true tls_version tlsv1.2 # on remplace le user / mot de passe par le certificat use_identity_as_username true allow_anonymous true</pre>	

Client mosquito : creation du certificat et configuration (déjà réalisé sur la VM debianProflot, à réaliser par les étudiants sur leurs VM)

Etape	Commande	remarques
-------	----------	-----------

# Sciences et Techniques Industrielles

Portail national de ressources - éduscol

Création de la clef (VM etudiant)	<code>etudiant@etudiantIot:~\$ openssl genrsa -out etudiant.key 2048</code>	Une clef est créée dans le fichier <code>etudiant.key</code> spécifié avec l'option <code>-out</code> Pas de mot de passe pour le client Donnée sensible (privée)
Créer une demande de certificat X509	<code>etudiant@etudiantIot:~\$ openssl req -new -key etudiant.key -out etudiant.csr</code> 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]:FR State or Province Name (full name) [Some-State]:Occitanie Locality Name (eg, city) []:Gragnague Organization Name (eg, company) [Internet Widgits Pty Ltd]:BTS CIEL Organizational Unit Name (eg, section) []: Common Name (e.g. server FQDN or YOUR name) []:etudiantIot Email Address []:  Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:etudiant An optional company name []:	En fluo, les réponses au script de création du certificat. En rouge : le nom doit correspondre au hostname  Ne pas mettre d'accents !  Une demande de certificat est créée dans le fichier <code>etudiant.csr</code>
Le client envoie sa demande de certificat à la CA	<code>etudiant@etudiantIot:~\$ scp etudiant.csr prof@debianProfIot:/home/prof/</code>	ou par FTP
La CA génère un certificat (.crt) à partir du CSR	<code>prof@debianProfIot:~\$ openssl x509 -req -in etudiant.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out etudiant.crt -days 365</code> Certificate request self-signature ok subject=C = FR, ST = Occitanie, L = Gragnague, O = BTS CIEL, CN = etudiantIot Enter pass phrase for ca.key:<mot de passe de la clef (prof)>	Manipulation à effectuer par le prof
Le client récupère son certificat	<code>etudiant@etudiantIot:~\$ scp prof@192.168.1.31:/home/prof/etudiant.crt .</code>	ou par FTP
Le client récupère le certificat de la CA	<code>etudiant@etudiantIot:~\$ scp prof@192.168.1.31:/home/prof/ca.crt .</code>	ou par FTP

# Sciences et Techniques Industrielles

Portail national de ressources - éduscol

A ce stade le client a quatre fichiers **etudiant.key**, **etudiant.csr** et **etudiant.crt + ca.crt**

Le fichier **etudiant.csr** peut être supprimé.

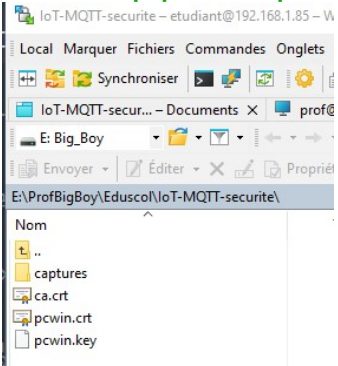
Commande MQTT en SSL	<pre>etudiant@etudiantIot:~\$ mosquitto_sub -h debianProfiot -t ciel -p 8883 --cafile ca.crt --cert etudiant.crt --key etudiant.key -d --tls-version tlsv1.2</pre> <p>Options :</p> <pre>--cafile : path/to/ca.crt --cert : path/to/certificate-client.crt --key : path/to/clefprivee-client.key -d : debug --tls-version : pour forcer la version tls (facultatif, à tester)</pre>	<p>Le hostname (<b>debianProfiot</b>) du broker doit impérativement correspondre au CN du certificat du broker</p> <p>Attention avant les options 'cafile', 'cert', 'key' et 'tls-version' il faut mettre deux tirets (<b>--</b>)</p>
----------------------	---	---

## Client Windows MQTTX : Création du certificat et configuration


Etape	Commande	remarques
Création de la clef (VM etudiant) Les fichiers sont créés sur la VM puis transférés sur Windows	<pre>etudiant@etudiantIot:~\$ openssl genrsa -out pcwin.key 2048</pre>	<p>Une clef est créée dans le fichier <b>pcwin.key</b> spécifié avec l'option -out</p> <p>Pas de mot de passe pour le client</p> <p>Donnée sensible (privée)</p>
Créer une demande de certificat X509	<pre>etudiant@etudiantIot:~\$ openssl req -new -key pcwin.key -out pcwin.csr</pre> <p>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]:<b>FR</b> State or Province Name (full name) [Some-State]:<b>Occitanie</b> Locality Name (eg, city) []:<b>Gragnague</b> Organization Name (eg, company) [Internet Widgits Pty Ltd]:<b>BTS CIEL</b> Organizational Unit Name (eg, section) []:<b>Windows</b> Common Name (e.g. server FQDN or YOUR name) []:<b>localhost</b> Email Address []:</p>	<p>En fluo, les réponses au script de création du certificat.</p> <p>En rouge : <b>localhost</b></p> <p>Ne pas mettre d'accents !</p> <p>Une demande de certificat est créée dans le fichier <b>pcwin.csr</b></p>

# Sciences et Techniques Industrielles

Portail national de ressources - éducol

	Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []: <b>pcwin</b> An optional company name []:	
Le client envoie sa demande de certificat à la CA	<b>etudiant@etudiantIot:~\$</b> scp pcwin.csr prof@debianProfIot:/home/prof/	ou par FTP
La CA génère un certificat (.crt) à partir du CSR	<b>prof@debianProfIot:~\$</b> openssl x509 -req -in <b>pcwin.csr</b> -CA <b>ca.crt</b> -CAkey <b>ca.key</b> -CAcreateserial -out <b>pcwin.crt</b> -days 365 Certificate request self-signature ok subject=C = FR, ST = Occitanie, L = Gragnague, O = BTS CIEL, OU = Windows, CN = localhost Enter pass phrase for ca.key:< <b>mot de passe de la clef (prof)</b> >	Manipulation à effectuer par le prof
Le client récupère son certificat	<b>etudiant@etudiantIot:~\$</b> scp prof@192.168.1.31:/home/prof/pcwin.crt .	ou par FTP
A ce stade le client a trois nouveaux fichiers pour le PC Windows <b>pcwin.key</b> , <b>pcwin.csr</b> et <b>pcwin.crt</b> Le fichier pcwin.csr peut être supprimé.		
Transfert des fichiers sur le PC Windows	<b>Par Winscp par exemple</b> 	ou par FTP
Configuration d'une connexion MQTTS sous M	Créer une nouvelle connexion MQTT (ou modifier la connexion précédente) en cochant SSL/TLS. Modifier le port en 8883. Le <b>hostname</b> du broker doit être le hostname défini dans le certificat du CA. Cocher « CA or Self-signed certificates » : trois champs apparaissent, où vous indiquez les chemins vers les fichiers de la clef privée du PC et des certificats.	Pour le hostname, si besoin ajouter le hostname dans le fichier hosts du PC.



[< Back](#)[Edit](#)[Connect](#) 

### General

\* Name

VM-brokerSSL

\* Host

mqtt://



debianProfiot

\* Port

8883

Client ID

mqttx\_pwin\_SSL

Username

Password

SSL/TLS

☒

SSL Secure

☒ ⓘ

ALPN


Certificate

☐ CA signed server certificate ☒ CA or Self signed certificates

### Certificates


CA File

E:\ProfBigBoy\Eduscol\IoT-MQTT-securite\ca.crt




Client Certificate File

E:\ProfBigBoy\Eduscol\IoT-MQTT-securite\pcwin.crt



Client key file

E:\ProfBigBoy\Eduscol\IoT-MQTT-securite\pcwin.key



### Advanced ▲

MQTT Version

5.0



Connect Timeout

10

  (s)