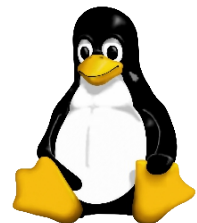
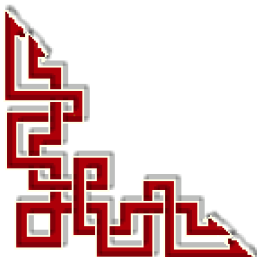


RF-232

Micronator

Serveur SME-9.1 & Certificat SSL



© **RF-232**
6447, avenue Jalobert, Montréal. Québec H1M 1L1

Tous droits réservés RF-232

AVIS DE NON-RESPONSABILITÉ

Ce document est uniquement destiné à informer. Les informations, ainsi que les contenus et fonctionnalités de ce document sont fournis sans engagement et peuvent être modifiés à tout moment. **RF-232** n'offre aucune garantie quant à l'actualité, la conformité, l'exhaustivité, la qualité et la durabilité des informations, contenus et fonctionnalités de ce document. L'accès et l'utilisation de ce document se font sous la seule responsabilité du lecteur ou de l'utilisateur.

RF-232 ne peut être tenu pour responsable de dommages de quelque nature que ce soit, y compris des dommages directs ou indirects, ainsi que des dommages consécutifs résultant de l'accès ou de l'utilisation de ce document ou de son contenu.

Chaque internaute doit prendre toutes les mesures appropriées (*mettre à jour régulièrement son logiciel antivirus, ne pas ouvrir des documents suspects de source douteuse ou non connue*) de façon à protéger le contenu de son ordinateur de la contamination d'éventuels virus circulant sur la Toile.

Toute reproduction interdite

Vous reconnaissez et acceptez que tout le contenu de ce document, incluant mais sans s'y limiter, le texte et les images, sont protégés par le droit d'auteur, les marques de commerce, les marques de service, les brevets, les secrets industriels et les autres droits de propriété intellectuelle. Sauf autorisation expresse de **RF-232**, vous acceptez de ne pas vendre, délivrer une licence, louer, modifier, distribuer, copier, reproduire, transmettre, afficher publiquement, exécuter en public, publier, adapter, éditer ou créer d'oeuvres dérivées de ce document et de son contenu.

Avertissement

Bien que nous utilisons ici un vocabulaire issu des techniques informatiques, nous ne prétendons nullement à la précision technique de tous nos propos dans ce domaine.

Sommaire

I-	Description générale.....	5
	1. Introduction.....	5
	2. Particularités de ce document.....	5
	3. Commentaires et suggestions.....	6
	4. Boutique de Micronator.....	6
II-	À savoir.....	7
	1. Usager(s) pour recevoir les courriels du certificat.....	7
	2. En cas de trouble majeur avec un certificat.....	8
	3. Paramètres.....	8
	4. Serveur virtuel de test.....	8
III-	Création de la requête CSR.....	9
	1. Introduction.....	9
	2. Création du répertoire de travail.....	10
	3. Nom du domaine (FQDN).....	11
	4. Notes pour la création d'une CSR.....	11
	5. Création de la requête CSR.....	12
IV-	Demander une certification à GoDaddy.....	14
	1. Page web de la demande de certificat SSL de GoDaddy.....	14
	2. Achat du certificat.....	14
	3. Configuration du certificat.....	15
	4. Courriel du certificat.....	16
	5. Téléchargement du certificat.....	17
	6. Désactivation du renouvellement automatique du certificat.....	17
V-	Réémission d'une certification GoDaddy.....	19
	1. Introduction.....	19
	2. Création de la requête CSR.....	19
	3. Login chez GoDaddy et gestion du certificat.....	19
VI-	Installation.....	23
	1. Introduction théorique.....	23
	2. Création d'un répertoire de travail.....	26
	3. Emplacement des fichiers du certificat actuel.....	26
	4. Sauvegarde des fichiers originaux.....	27
	5. Copie des nouveaux fichiers vers le répertoire de travail.....	29
	6. Installation des fichiers du nouveau certificat.....	29
VII-	Vérification.....	33
	1. Vérification avec Firefox.....	33
	2. Vérification avec Google Chrome.....	36

3.	Vérification avec l'Explorateur Internet de Microsoft.....	37
4.	Vérification avec le navigateur TOR.....	38
5.	Sceau de sécurité.....	40
VIII-	Demander une certification à Namecheap.....	43
1.	Introduction.....	43
2.	Choix du certificat & création d'un compte.....	44
3.	Paieement.....	45
4.	Activation du certificat.....	46
5.	Copie du contenu de la requête.....	47
6.	Courriel et validation du certificat.....	50
7.	Réception du certificat.....	50
8.	Vérification du statut du certificat.....	51
9.	Installation du certificat.....	51
IX-	Réémission d'une certification Namecheap.....	52
1.	Introduction.....	52
2.	Création du fichier pour la requête CSR.....	52
3.	Réémission.....	52
4.	Aide en ligne chez namecheap.com.....	57
X-	Création d'un certificat SME standard.....	58
1.	Introduction.....	58
2.	Création d'un répertoire de sauvegarde.....	58
3.	Sauvegarde des fichiers du certificat actuel.....	59
4.	Effaçage des fichiers du certificat.....	60
5.	Signalement des modifications et réamorçage.....	61
6.	Vérification.....	61
	Crédits.....	63

I- Description générale

1. Introduction

Ce document explique la marche à suivre pour installer un certificat **SSL** sur un **Serveur SME-9.1** roulant **WordPress** avec l'extension **WooCommerce**. Ce certificat est requis pour les paiements avec l'extension **Stripe for WooCommerce**.

Nous allons créer deux requêtes **CSR**, installer et vérifier deux certificats: un émis par **GoDaddy.com** et un autre par **namecheap.com**.

2. Particularités de ce document

2.1. Notes au lecteur

* Les captures d'écrans ne sont que des références.

** Les informations écrites ont préséance sur celles retrouvées dans les captures d'écrans. Veiller à se référer aux différents tableaux lorsque ceux-ci sont présents.

2.2. Conventions

Toutes les commandes à entrer à la console sont en **gras**. Les affichages à surveiller sont en **rouge**, **bleu**, **orange** ou **magenta**.

```
# ping 192.168.1.149
192.168.1.149 is alive
#
```

Les liens de référence Internet sont en **bleu** et ceux intra document en **bleu**.



Manipulation, truc ou ruse pour se tirer d'embarras.



Une recommandation ou astuce.



Une note.



Une étape, note ou procédure à surveiller.



Paragraphe non complété ou non vérifié.



Cette icône indique que cette commande est sur une seule ligne. Le **PDF** la mettra sur deux lignes avec un **[CR]** **[LF]** entre les deux. Il faudra donc copier la commande entière dans un éditeur de texte ASCII et la mettre sur une seule ligne avant de la copier à la console.

3. Commentaires et suggestions

RF-232 apprécie énormément échanger avec ses internautes. Vos commentaires et suggestions sont indispensables à l'amélioration de la documentation et du site **micronator.org**.

N'hésitez pas à nous transmettre vos commentaires et à nous signaler tout problème d'ordre technique que vous avez rencontré ou n'arrivez pas à résoudre. Tous vos commentaires seront pris en considération et nous vous promettons une réponse dans les plus brefs délais.



**Brancher les aînés,
encourager l'Informatique Libre
et la diffusion du savoir**



4. Boutique de Micronator

Nous sommes heureux de vous présenter notre nouvelle boutique en ligne sur laquelle vous trouverez certains de nos produits qui ne sont pas disponibles sur notre site principal. Nous vous laissons le plaisir de parcourir notre boutique. [Allez à l'accueil de notre boutique.](#)

Faites votre choix, remplissez votre panier et réglez votre commande avec la carte bancaire de votre choix, **MasterCard, Visa, Discover, American Express**, etc...

Il n'est pas nécessaire d'ouvrir un compte **PayPal**. Vous pouvez choisir la carte bancaire que vous désirez. [Cliquez ici](#) pour voir les étapes de paiements. Les paiements sont sécurisés par le système **PayPal**.

II- À savoir

1. Usager(s) pour recevoir les courriels du certificat

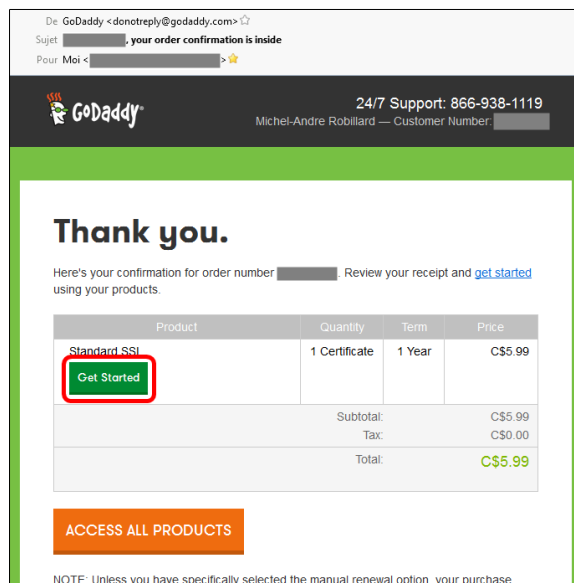
1.1. Certificat GoDaddy.com

1.1.1. Code de validation

C'est l'usager titulaire du compte chez **GoDaddy.com** qui recevra le premier courriel, lors de l'achat. Ce courriel contient un lien **Get Started** qu'on clique pour accéder à la gestion du certificat.

⚠ Ce n'est qu'après cette gestion que le certificat sera envoyé par courriel.

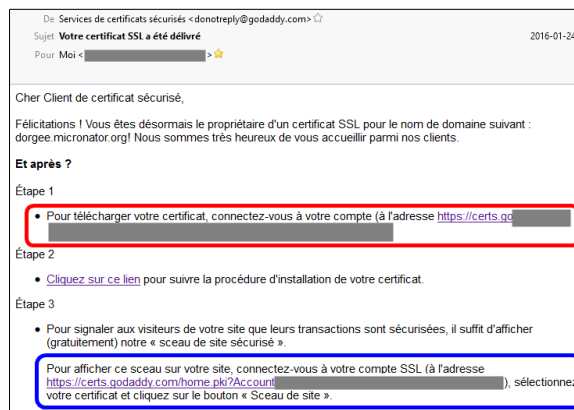
⚠ Il faut que l'adresse courriel du titulaire du compte appartienne au domaine pour lequel on demande le certificat. C'est de cette façon que l'émetteur du certificat vérifie que le domaine spécifié existe vraiment.



1.1.2. Fichier ZIP du certificat

C'est l'usager titulaire du compte chez **GoDaddy.com** qui recevra le deuxième courriel. Ce courriel contiendra un lien qu'on cliquera pour télécharger le certificat.


Un autre lien est disponible, dans l'encadré bleu, pour se procurer un sceau de sécurité à afficher sur le site pour signaler aux visiteurs que leurs transactions sont sécurisées; ce sceau est gratuit. Voir le paragraphe [Sceau de sécurité](#) à la page [40](#).



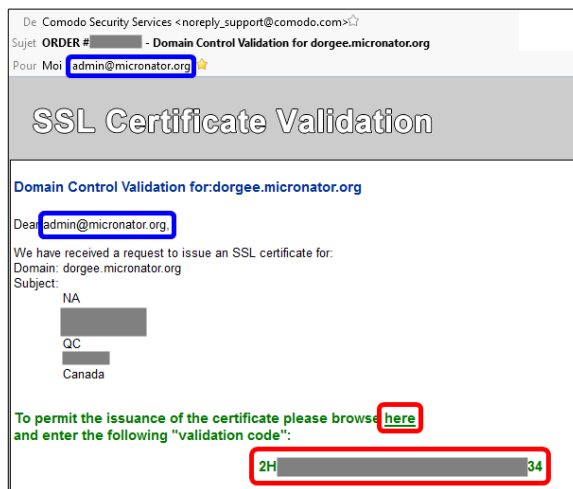
1.2. Certificat namecheap.com

1.2.1. Code de validation

C'est l'utilisateur **admin** (exemple: *admin@nom-du-domaine*) du **Serveur SME** qui recevra le premier courriel de l'émetteur du certificat. Ce courriel contient un lien et un code de validation "**validation code**". Il faut copier ce "**validation code**", cliquer sur le lien [here](#) contenu dans le courriel et coller ce code dans la page que le lien va ouvrir.

 Ce n'est qu'après cette validation que le certificat sera envoyé par courriel.

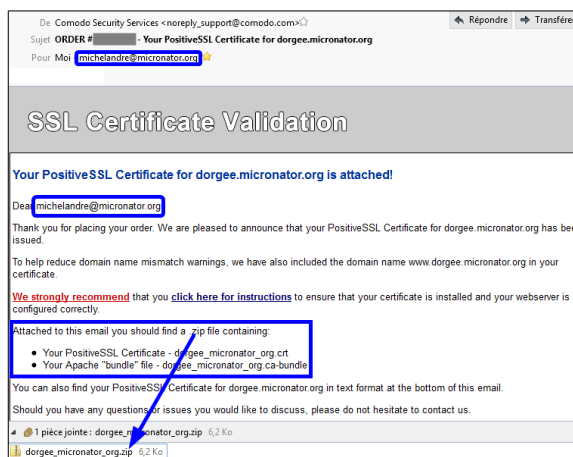
C'est de cette façon que l'émetteur du certificat vérifie que le domaine spécifié existe vraiment.



1.2.2. Fichier ZIP du certificat

C'est l'utilisateur qui est titulaire du compte chez **namecheap.com** qui recevra le courriel contenant le **fichier ZIP** du certificat envoyé par l'émetteur (*comodo.com*).

Le titulaire du compte chez **namecheap.com** peut avoir une autre adresse courriel que **admin@nom-du-domaine**.



2. En cas de trouble majeur avec un certificat

Advenant un trouble majeur avec un certificat et qu'on veuille en recréer un original, émis et certifié par le **Serveur SME** lui-même, veuillez vous référer au paragraphe: [Création d'un certificat SME standard](#) à la page [58](#).

3. Paramètres

Une **chaîne de caractères en magenta** indique qu'il faut remplacer cette chaîne par vos propres paramètres

4. Serveur virtuel de test

Si nous voulons commencer par l'installation du certificat sur un serveur virtuel de test et ainsi ne rien risquer sur le serveur réel, voir: http://www.micronator.org/?page_id=2437.

III- Création de la requête CSR

1. Introduction

Référence: https://fr.wikipedia.org/wiki/Demande_de_signature_de_certificat.

Dans une infrastructure **PKI** (*Public Key Infrastructure soit infrastructure à clés publiques*), une demande de signature de certificat (*CSR pour Certificate Signing Request*) est un message envoyé à partir d'un demandeur à une autorité de certification afin de demander un certificat d'identité numérique. Le format le plus commun pour les CSR est la spécification **PKCS#10**.

1.1. Procédure

Avant de créer une **CSR**, le requérant crée une paire de clés (*une publique et une privée*) en gardant la clé privée secrète. La **CSR** contient des informations d'identification du demandeur (*examiné comme un nom unique dans le cas d'un certificat X.509*) et la clé publique choisie par le demandeur. La clé privée correspondante n'est pas incluse dans la **CSR**, mais est utilisée pour signer numériquement la demande. La **CSR** peut être accompagnée par d'autres informations d'identification ou des preuves d'identité requises par l'autorité de certification; l'autorité de certification peut contacter le demandeur pour plus d'informations.

Si la demande est acceptée, l'autorité de certification retourne un certificat d'identité signé numériquement avec la clé privée de l'autorité de certification.

Voici les informations typiquement présentes dans une **CSR**:





Les informations entre parenthèses dans la colonne **Information** constituent une fois assemblées le nom complet qui sera employé dans le certificat.

Information	Description
Common Name (CN=)	Le nom complet (FQDN) du domaine Internet à sécuriser par exemple "www.micronator.org" ¹ .
Nom de l'entreprise / Organisation (O=)	Nom d'une société ou d'une association légalement constituée.
Nom du département / Unité Organisationnelle (OU=)	Par exemple Micronator, RH, finance, informatique
Localité (L=)	Par exemple Montreal ² , Paris, Londres
Province, Région ou État (S=)	Par exemple QC, Qc, Quebec ² , Ile-de-France
Pays (C=)	Le code à deux lettres ISO pour le pays où est situé l'organisme. Par exemple CA, FR
Une adresse courriel	Une adresse courriel pour contacter l'organisation ³ . Habituellement l'adresse courriel de l'administrateur de certificats

¹ Il est possible de sécuriser plusieurs domaines grâce à l'emploi du caractère joker * comme dans "*.wikipedia.org" qui englobe toutes les langues de Wikipédia.

² La saisie d'informations n'accepte pas les caractères suivants: <>~!@# \$%^*\/\() ? & **et les accents**.

³ Chez **GoDaddy**, tout est envoyé au titulaire du compte **GoDaddy**. Chez **namecheap.com**, la validation de l'achat du certificat est envoyé à l'utilisateur **admin** du serveur et la clé au titulaire du compte **namecheap.com**.

  Si vous avez choisi d'avoir un mot de passe sur votre clé privée, **vous serez invité à l'entrer à chaque fois qu'Apache est démarré ou redémarré. Apache ne démarre pas pleinement** jusqu'à ce que le mot de passe soit entré. Un message sera affiché en boucle à la console du serveur.

2. Création du répertoire de travail

On se logue à la console du serveur avec **PuTTY**.

```
login as: root

root@192.168.1.201's password:
Last login: Mon Jan 18 07:58:02 2016
***** Welcome to SME Server 9.1 *****

Before editing configuration files, familiarise
yourself with the automated events and templates
systems.

Please take the time to read the documentation
http://wiki.contribs.org/Main_Page

Remember that SME Server is free to download
and use, but it is not free to build

Please help the project :
http://wiki.contribs.org/Donate

*****
[root@dorgee ~]#
```

On vérifie qu'on est bien dans le répertoire de l'utilisateur **root**.

```
[root@dorgee ~]# pwd

/root
[root@dorgee ~]#
```

On crée un répertoire pour la génération de la requête.

```
[root@dorgee ~]# mkdir CSR

[root@dorgee ~]#
```

On vérifie.

```
[root@dorgee ~]# ls -alsd CSR

4 drwxr-xr-x 2 root root 4096 18 janv. 16:54 CSR
[root@dorgee ~]#
```

On entre dans le répertoire.

```
[root@dorgee ~]# cd CSR

[root@dorgee CSR]#
```

On vérifie.

```
[root@dorjee CSR]# pwd
/root/CSR
[root@dorjee CSR]#
```

3. Nom du domaine (FQDN)


On affiche le fichier `/etc/hosts` pour s'assurer du nom exact de notre **Serveur SME (FQDN)**.

```
[root@dorjee CSR]# cat /etc/hosts
#-----
#
#           !!DO NOT MODIFY THIS FILE!!
#
# Manual changes will be lost when this file is regenerated.
#
# Please read the developer's guide, which is available
# at http://www.contribs.org/development/
#
# Copyright (C) 1999-2006 Mitel Networks Corporation
#-----
127.0.0.1          localhost
10.10.100.38      dorjee.micronator.org dorjee
[root@dorjee CSR]#
```

4. Notes pour la création d'une CSR

L'entrée par défaut pour "Country Name" entre [] est **XX**. Entrer le code de deux lettres de votre pays.

Vous devez entrer les autres valeurs. Toutes ces valeurs devraient être explicites mais vous devez suivre ces lignes directrices:

- La saisie d'informations n'accepte pas les caractères suivants: `<>~!@#$%^*\/() ? & et les accents`.
 - Ne pas abrégier le nom de la localité ou de l'état. Les écrire au complet (*par exemple, St-Denis doit être noté Saint-Denis*).
 - Si vous envoyez la **CSR** à une autorité (*CA*), soyez très attentif à fournir des informations correctes pour tous les champs mais surtout pour les noms **Organization Name** et **Common Name**. La *CA* vérifie les informations fournies dans la **CSR** afin de déterminer si votre organisation est bien celle dont vous avez fourni le **Common Name**. La *CA* rejette les **CSR** qui contiennent des information qu'il perçoit comme non valide.
 - Pour **Common Name**, assurez-vous que vous tapez le nom réel de votre domaine sécurisé (*un nom **DNS** valide*) et non pas un alias que le serveur pourrait avoir.
 - L'adresse courriel doit être celle du webmestre ou celle de l'administrateur du système (*admin*).
 - Évitez les caractères spéciaux tels `@, #, &, !, les accents`, etc. Certaines *CA* rejettent une demande de certificat qui contient un caractère spécial. Donc, si votre nom de société comprend une esperluette (`&`), entrez `"et"` au lieu de `"&"`.
-  • N'utilisez aucun des attributs supplémentaires ("Challenge password" et "An optional company name"). Pour continuer sans entrer ces champs, appuyez simplement sur [Entrée] pour accepter la valeur vide par défaut pour les deux entrées.

4.1. Nom Commun (CommonName)

Référence:

<https://ca.godaddy.com/fr/help/generer-une-demande-de-signature-de-certificat-csr-pour-iis-7-4800>.

La saisie d'informations n'accepte pas les caractères suivants: <>~!@#\$\$%^*\/\()\? & **et les accents**.

Nom commun – Nom de domaine complet (*FQDN*) ou **URL** auquel vous avez prévu d'associer ce certificat (*il s'agit de la zone de votre site à laquelle vous souhaitez que les visiteurs se connectent en mode SSL*).



Il est recommandé de débiter le nom du domaine par **www** (ex: **www.micronator.org**).

Un certificat **SSL** émis pour **www.coolexample.com** ne sera pas valide pour **secure.coolexample.com**. Si vous souhaitez que votre certificat **SSL** couvre **secure.coolexample.com**, assurez-vous que le **Nom Commun** soumis dans la demande **CSR** est **secure.coolexample.com**.

Si vous demandez un certificat générique, ajoutez un astérisque (*) à gauche du **Nom Commun** (par exemple, ***.coolexample.com** ou ***.secure.coolexample.com**).

5. Création de la requête CSR

Référence: <https://ca.godaddy.com/fr/help/generation-dune-demande-de-signature-de-certificat-5343>.



Le nom de notre domaine est: **micronator.org** donc le **Nom Commun** (*CommonName*) sera **www.micronator.org**. Ce préfixe facilitera les connexions pour les clients courriels.



Il est recommandé d'entrer le nom du serveur dans la commande qui génère la requête i.e. **dorgee.micronator.org.key** et **dorgee.micronator.org.csr** qui sont les noms des fichiers de sortie de la commande. Plus tard, il ne sera pas nécessaire de tous les renommer.



Si vous avez choisi d'avoir un mot de passe sur votre clé privée, **vous serez invité à l'entrer à chaque fois qu'Apache est démarré ou redémarré**. **Apache ne démarrera pas pleinement** jusqu'à ce que le mot de passe soit entré. Un message sera affiché en boucle à la console du serveur.

On génère la requête pour un certificat **RSA** de **2048 bits**.



```
[root@dorgee CSR]# openssl req -newkey rsa:2048 \
                        -nodes \
                        -keyout dorgee.micronator.org.key \
                        -out dorgee.micronator.org.csr

Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'dorgee.micronator.org.key'
-----
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) [XX]:CA
State or Province Name (full name) []:QC
Locality Name (eg, city) [Default City]:Montreal
Organization Name (eg, company) [Default Company Ltd]:RF-232
Organizational Unit Name (eg, section) []:Micronator
Common Name (eg, your name or your server's hostname) []:www.micronator.org
Email Address []:michelandre@micronator.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@dorgee CSR]#
```

Création de la requête CSR

On vérifie les fichiers.

```
[root@dorgee CSR]# ls -als
total 16
4 drwxr-xr-x 2 root root 4096 18 janv. 17:05 .
4 dr-xr-x--- 7 root root 4096 18 janv. 16:54 ..
4 -rw-r--r-- 1 root root 1074 18 janv. 17:05 dorgee.micronator.org.csr
4 -rw-r--r-- 1 root root 1704 18 janv. 17:05 dorgee.micronator.org.key
[root@dorgee CSR]#
```

Le fichier **dorgee.micronator.org.csr** est celui utilisé pour la requête CSR.



Le fichier **dorgee.micronator.org.key** est la **clé privée du Serveur SME**. Ce fichier est extrêmement confidentiel car c'est cette clé qui sert à déchiffrer tous nos messages.

On vérifie le fichier pour notre requête.

```
[root@dorgee CSR]# cat dorgee.micronator.org.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC4TCCAckCAQAwZSxCzAJBgNVBAYTAkNBAAswCQYDVQQIDAJRQzERMA8GA1EU
BwwITW9udHJlYWwxdzANBgNVBAoMB1JGLTIzMjETMBEGA1UECwwKTWljcm9uYXVr
...
...
...
VU2YOhPGj3LUUP8pJTXWdwCEzid4UHFN7stJ6OvjcXre/beDEmocwdsydXAcRc6
kIgZ4Y1SoPS2CA1MNxTmibfdDLnHw+hXjFYCs+ocVmh4ysqMTrXpFKiW1GpFZHST
tfnfa137mm2VpZIW86pj5ICg/JWq
-----END CERTIFICATE REQUEST-----
[root@dorgee CSR]#
```

On est prêt à faire notre requête auprès d'une autorité de certification.

IV- Demander une certification à GoDaddy

1. Page web de la demande de certificat SSL de GoDaddy

On se rend à la page: https://ca.godaddy.com/offers/default.aspx?gclid=CNTIvb6AyMoCFYU9aQodJosEWw&isc=ssh15ca24&tmskey=1ssl_5&pcode=310211712¤cytype=CAD&cvosrc=ppc.google.godaddy%20ssl%20certificate&cvo_crid=77286718038&matchtype=e&ef_id=VqetBgAABNfSIDBS:20160126172942:s

Ou recherche dans Google: *godaddy ssl certificate*

\$5.99 GoDaddy SSL - Secure Your Website in Minutes
 Annonce ca.godaddy.com/SSLCertificate
 Free Dedicated 24/7 Support.
 Award-winning customer service - Stevie Awards.
 \$0.99 .com Sale - \$1.49/Mth Web Hosting - CA Domain Registration

2. Achat du certificat

Add to Cart.

On vérifie | Proceed to Checkout.

- Si on n'a pas de compte GoDaddy, cliquer **Continuer**.

- On entre les informations demandées | **Log in**.

Lire *Universal Terms of Service Agreement, Private Policy* et *Hosting Agreement*. Si on accepte, on coche, on vérifie | **Proceed to Checkout**.

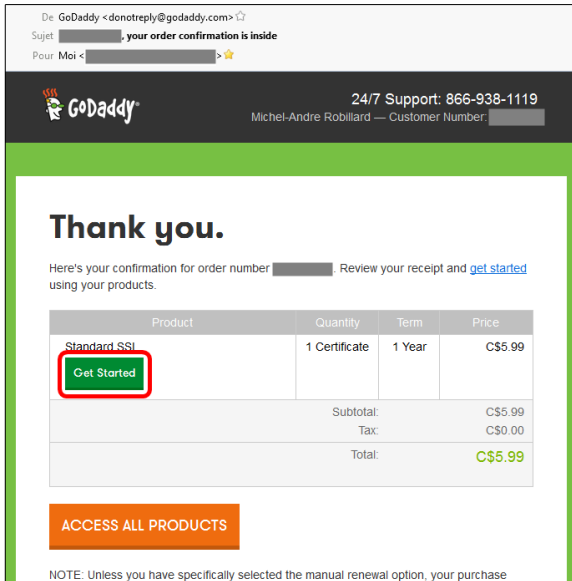
Ce certificat sera automatiquement renouvelé à un prix différent beaucoup plus dispendieux.



On peut changer ce renouvellement pour qu'il soit manuel. Voir le paragraphe *Désactivation du renouvellement automatique du certificat* à la page 17.

3. Configuration du certificat

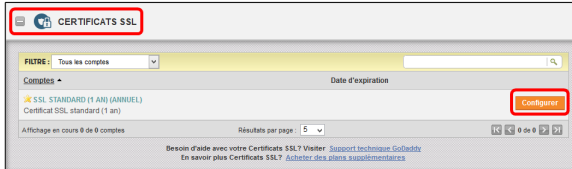
Get Started.



On entre les informations demandées | **Se connecter.**



On clique **CERTIFICATS SSL** pour afficher le produit | **Configurer.**



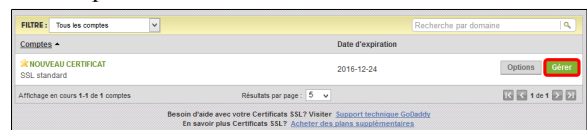
Configurer.



Le **Certificat SSL** a été ajouté avec succès.



On clique **Gérer.**



Dans **PuTTY**, à la console du **Serveur SME-9.1**, on affiche le fichier de notre requête avec la commande **cat**.

```
[root@dorgée CSR] # cat wwwmicronator.org.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC4TCCAckCAQAwgZsxCzAJBgNVBAYTAkNBAAswCQYDVQQIDAJRQzERMA8GA1EU
BwwITW9udHJlYWwxdzANBgNVBAoMB1JGLTIzMjETMBEGA1UECwwKRWljbW9uYXVX
...
kIgZ4Y1SoPS2CA1MNxTmibfdDlnHw+hXjFYCs+ocVmh4ysqMTxXpFKiW1GpFZHST
tfnfa137mm2VpZIW86pj5ICg/JWq
-----END CERTIFICATE REQUEST-----
[root@dorgée CSR] #
```

! On sélectionne tout entre **BEGIN** et **END**, on copie (avec **[CTL] + [c]**) incluant les lignes entières **BEGIN** et **END**. Il ne faut pas de lignes vides avant ou après **BEGIN** et **END**.

On colle dans le cadre, on choisit **GoDaddy SHA-2**, on coche **Contact...** et **Adresses électroniques...**, on lit les **Conditions générales du Contrat d'abonnement** et on coche si on les accepte puis **Demander un certificat**.

1 année Certificat SSL standard
Installation du certificat

Sélectionnez un site Web

Fournissez une demande de signature de certificat (CSR)

Signature de certificat (CSR) [En savoir plus](#)

```
-----BEGIN CERTIFICATE REQUEST-----
ZzeCscwMnS6Y4QsdSMcaqCMJjp
/If5DWOmEogbFPwQRHTz3EjaSMrm7orIZ9xvly
rptgsGj6CSQXmG7aTA3Mjy5pdmfhdqMz
-----END CERTIFICATE REQUEST-----
```

Nom de domaine (basé sur le CSR) : **dorgee.micronator.org**

Propriété du domaine

Nous enverrons un mail avec un code unique à l'adresse enregistrée. Suivez ses instructions pour vérifier que vous disposez du contrôle du site Web ou DNS sur le domaine sélectionné. [Plus d'informations](#)

ET

Nous pouvons envoyer les mails d'instruction sur la propriété de domaine à l'un ou à tous les destinataires suivants :

- Contacts répertoriés dans l'enregistrement de base de données WHOIS publique du domaine
- Adresses électroniques : admin@[domain], administrator@[domain], hostmaster@[domain], postmaster@[domain], et webmaster@[domain]

[Masquer les options avancées](#)

Algorithme de signature [En savoir plus](#)

GoDaddy SHA-2

J'accepte les Conditions générales de [Contrat d'abonnement](#)

Demander un certificat Annuler

Rien à faire jusqu'à la réception du courriel de **GoDaddy** qui inclura un fichier **ZIP** de notre certificat et du fichier de la chaîne de certification.

VÉRIFICATION DE LA PROPRIÉTÉ DE DOMAINE POUR LES DEMANDES DE CERTIFICATS SSL (HTML OU DNS)

Lorsque vous demandez un certificat SSL, nous pouvons vous demander de vérifier que vous possédez bien l'URL pour laquelle vous demandez un certificat. Pour ce faire, nous vous proposons une des deux options suivantes :

Méthode	Fonctionnement
Page HTML	Chargez une page HTML avec le contenu que nous spécifions dans le répertoire le plus élevé du site Web du nom commun que vous utilisez
Enregistrement DNS	Créez un enregistrement TXT que nous spécifions dans le fichier de zone (DNS) de votre nom de domaine

Le type de vérification que vous pouvez utiliser dépend du type de certificat que vous demandez :

Type de certificat	HTML	DNS
Standard	✓	✓
Deluxe	✓	✓
Validation étendue	✓	-
Générique	-	✓
UCC	✓	✓

Cliquez sur l'un des liens suivants pour des instructions en fonction des informations que nous vous avons fait parvenir par mail.

- [Page HTML](#)
- [Enregistrement DNS](#)

Après avoir chargé la page HTML ou créé l'enregistrement TXT, vous devez nous le faire savoir afin que nous puissions vérifier la propriété de votre nom de domaine.

- Pour vérifier la propriété de votre nom de domaine**
 - Connectez-vous et rendez-vous dans la section Chargé de compte.
 - Cliquez sur **Certificats SSL**.
 - En face du certificat que vous souhaitez utiliser, cliquez sur **Gérer**.
 - En face du certificat que vous souhaitez utiliser, dans la colonne **Actions**, cliquez sur **Afficher le statut**.
 - Cliquez sur **Vérifier ma mise à jour**.

La vérification peut prendre de 5 à 10 minutes.

Cet article était-il utile ?

4. Courriel du certificat

On se logue à **WebMail**, avec le nom de l'utilisateur du compte **GoDaddy**, à <https://notre-domaine/webmail> et on affiche le courriel reçu de **GoDaddy**.

On clique sur le lien pour télécharger notre fichier **zip** du certificat.

Chez **GoDaddy** | **Mes produits** | on clique certificat pour dérouler | **Gérer**.

CERTIFICATS SSL

FILTRE : Tous les comptes Recherche par domaine

Comptes	Date d'expiration
www.micronator.org SSL standard	2017-01-24

Affichage en cours 1-1 de 1 comptes Résultats par page 5

Besoin d'aide avec votre Certificat SSL? Visitez [Support technique GoDaddy](#)
En savoir plus Certificat SSL? [Acheter des plans supplémentaires](#)

De: Services de certificats sécurisés <donotreply@godaddy.com>

Sujet: **Votre certificat SSL a été délivré**

Pour: Moi <[redacted]>

Étape 1

- Pour télécharger votre certificat, connectez-vous à votre compte** (à l'adresse <https://certs.godaddy.com>).

Étape 2

- [Cliquez sur ce lien](#) pour suivre la procédure d'installation de votre certificat.

Étape 3

- Pour signaler aux visiteurs de votre site que leurs transactions sont sécurisées, il suffit d'afficher (gratuitement) notre « sceau de site sécurisé ».

Pour afficher ce sceau sur votre site, connectez-vous à votre compte SSL (à l'adresse [https://certs.godaddy.com/home.pk?AccountId=\[redacted\]](https://certs.godaddy.com/home.pk?AccountId=[redacted])), sélectionnez votre certificat et cliquez sur le bouton « Sceau de site ».

Si vous rencontrez des difficultés ou si vous avez des questions, n'hésitez pas à nous contacter. Nous sommes à votre écoute 24x7.

Service clientèle :
Mail : ra@godaddy.com
Tél : 09 75 18 70 39
Fax : +1 480 393 5009

Pour plus de détails, connectez-vous à votre compte : <https://certs.godaddy.com>

Sans vouloir abuser de votre temps, nous serions très heureux de lire vos réponses à cette petite [enquête](#), qui nous permettra de connaître votre opinion sur les opérations effectuées jusqu'à présent. Nous pouvons vous

5. Téléchargement du certificat

Télécharger.

Tout > www.micronator.org
Certificat SSL standard

Options de gestion des certificats

Télécharger Gérer

Détails du certificat

Statut	Certificat émis (Révoquer)
Nom de domaine	www.micronator.org
Puissance du cryptage	GoDaddy SHA-2
Période de validité	2016-1-27 - 2017-1-24
Numéro de série	a1:2f4cfcf6bd7:50:6b

Type de serveur Apache | Télécharger le fichier Zip.

www.micronator.org > Télécharger le certificat
Certificat SSL standard

Pour sécuriser votre site s'il est hébergé ailleurs, téléchargez le fichier Zip correspondant à votre type de serveur d'hébergement. Installez ensuite toutes les certificats du fichier Zip sur votre serveur d'hébergement, y compris tous les certificats intermédiaires éventuellement nécessaires pour les navigateurs et les serveurs anciens.

C'est la première fois que vous installez un certificat ? [Afficher les instructions d'installation du serveur sélectionné.](#)

Type de serveur
Apache

Télécharger le fichier Zip Annuler

On sauvegarde le fichier **ZIP** du certificat dans un endroit sécuritaire après l'avoir dézippé.

Nom	Modifié le	Type	Taille
abcdef3sm27i0nm2b7xyocabcdefg.zip	2016-01-24 16:14	Dossier compressé	5 Ko
bcc6e126a86ab22f.crt	2016-01-24 14:13	Certificat de sécurité	2 Ko
gd_bundle-g2-g1.crt	2016-01-24 14:13	Certificat de sécurité	5 Ko

6. Désactivation du renouvellement automatique du certificat

Chez **GoDaddy**, on clique notre nom d'utilisateur | **Mes produits** | on clique **CERTIFICAT SSL** pour le dérouler | **Options**.

Chez **GoDaddy**, on clique notre nom d'utilisateur | **Mes produits**.

AIDE [Avatar] ✓

Informations client

Michel-Andre Robillard
N° de client: 3275100

Mes produits

On clique **CERTIFICAT SSL** pour dérouler | **Options**.

CERTIFICATS SSL

FILTRE: Tous les comptes Recherche par domaine

Comptes	Date d'expiration
www.micronator.org SSL standard	2017-01-24

Affichage en cours 1-1 de 1 comptes Résultats par page: 5

Besoin d'aide avec votre Certificats SSL? Visitez [Support technique GoDaddy](#)
En savoir plus Certificats SSL? [Achetez des plans supplémentaires](#)

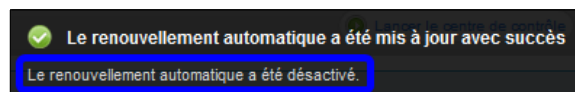
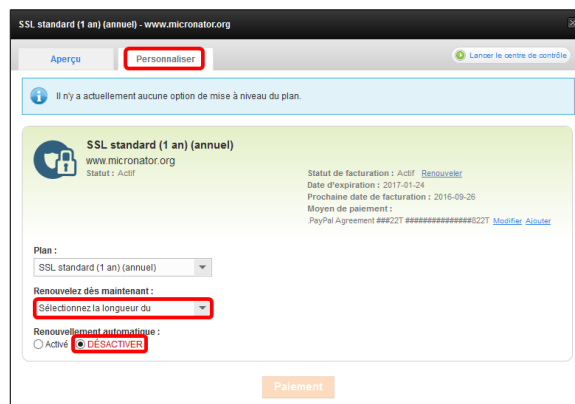
On clique l'onglet **Personnaliser**.

On déroule **Renouvellement dès maintenant**: et on choisit **Sélectionnez la longueur du** et enfin on clique **DÉSACTIVER**.

Une fenêtre apparaît quelques secondes affichant *Le renouvellement automatique a été désactivé.*

On ferme la fenêtre en cliquant le **X**, en haut à droite.

Nous sommes prêts à installer le nouveau certificat sur notre **Serveur SME9.1**.



V- Réémission d'une certification GoDaddy

1. Introduction

Plusieurs problèmes peuvent vous amener à devoir faire une demande de réémission de **certificat SSL**.

- Perte de votre clé privée.
- Changement de serveur.
- etc...

Dans de telles situations, il n'est pas nécessaire d'acheter un nouveau certificat. Une simple réémission du certificat est possible.

Par contre, cette réémission de certificat conserve sa date d'expiration d'origine. Si votre **certificat SSL** d'origine d'une durée de 1 an devait expirer le 1er juin 2016, sa réémission le 12 avril 2016 conserverait la même date d'expiration du 1er juin 2016.

On peut renouveler gratuitement un certificat émis par **GoDaddy**.

2. Création de la requête CSR

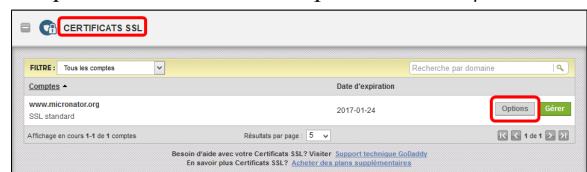
On doit créer de nouveaux fichiers de requête, **.csr** et **.key**, pour une réémission. On utilise la même manière que la procédure décrite au paragraphe [Création de la requête CSR](#) à la page [12](#), sans oublier le paragraphe [Notes pour la création d'une CSR](#) à la page [11](#), afin de générer une nouvelle demande de signature de certificat.

3. Login chez GoDaddy et gestion du certificat

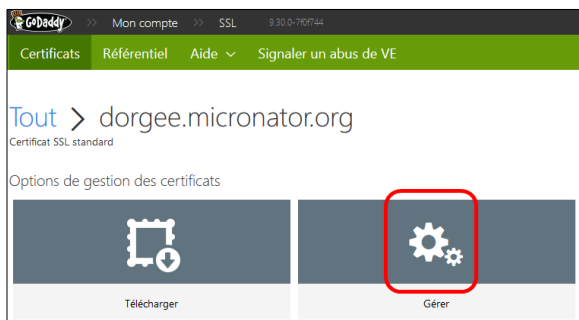
- Cliquer **Se connecter** pour faire apparaître le menu.
- Entrer les informations demandées.
- **SE CONNECTER**.



On clique notre nom d'utilisateur | **Mes produits** | on clique **CERTIFICAT SSL** pour dérouler | **Gérer**.



Gérer.

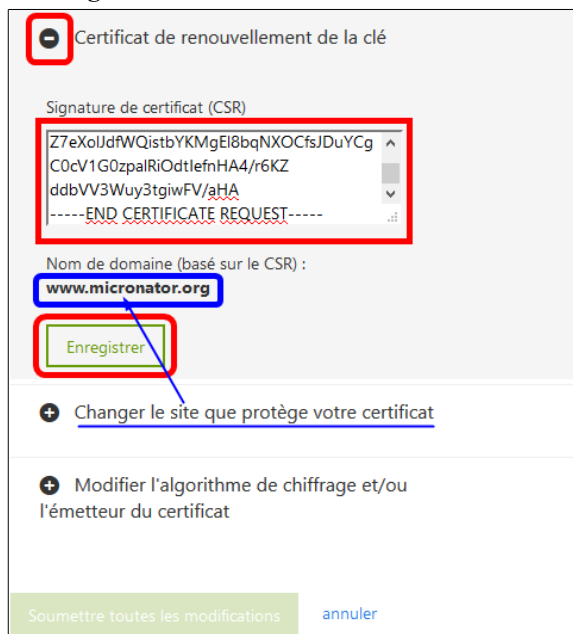


La ligne ci-contre soulignée en **bleu**, **Changer le site que protège votre certificat**, est utile si on veut modifier le nom de domaine.

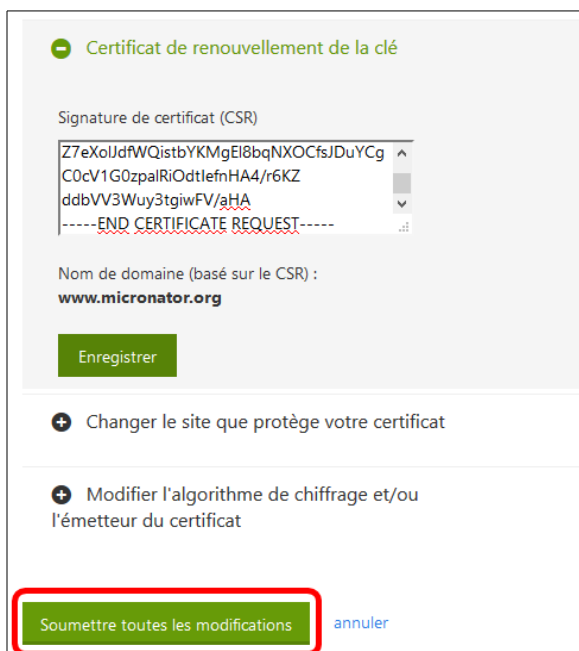


Exemple: si nous avons **dorgee.micronator.org** et que nous voulions modifier ce nom de domaine pour **www.micronator.org**, c'est sur cette ligne qu'il faudrait cliquer.

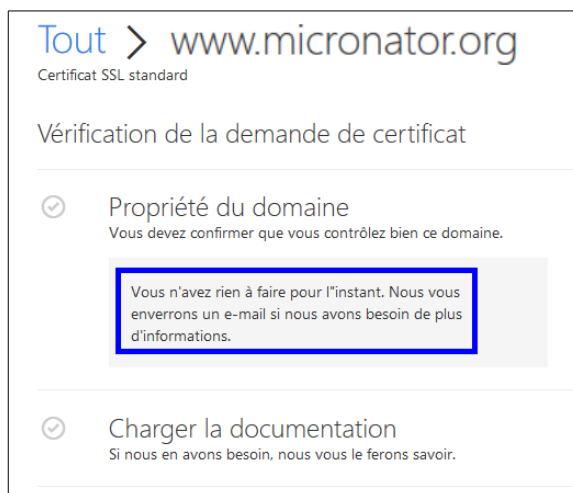
- Cliquer sur le + pour dérouler.
- Coller le contenu du fichier généré par la CSR dans le cadre **Signature de certificat (CSR)**.
- **Enregistrer.**



Soumettre toutes les modifications.



On a rien à faire.

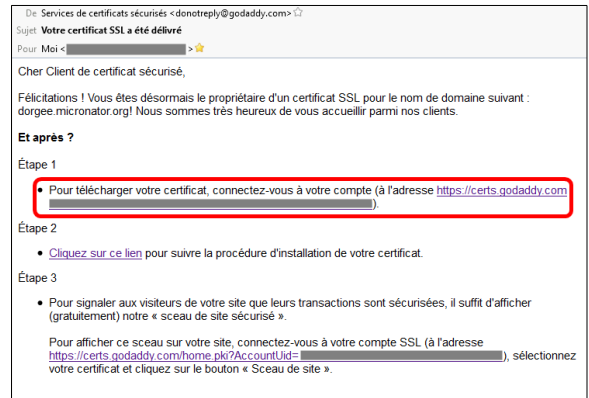


Réémission d'une certification GoDaddy

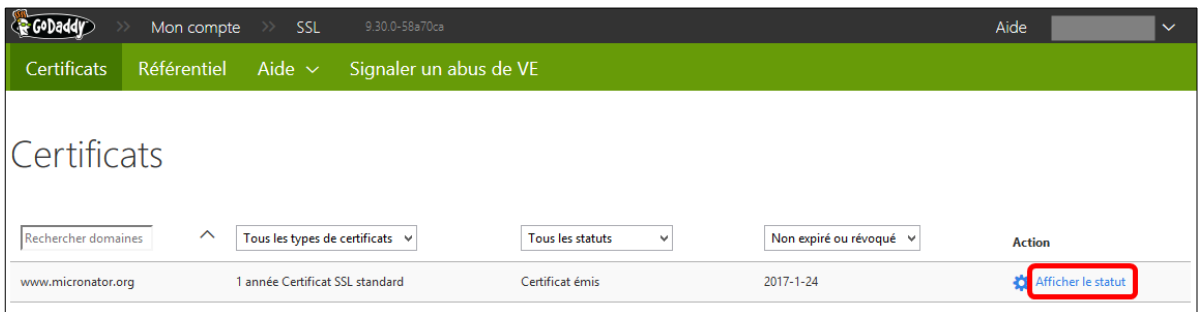
Après quelques minutes le statut change pour **Terminé**.



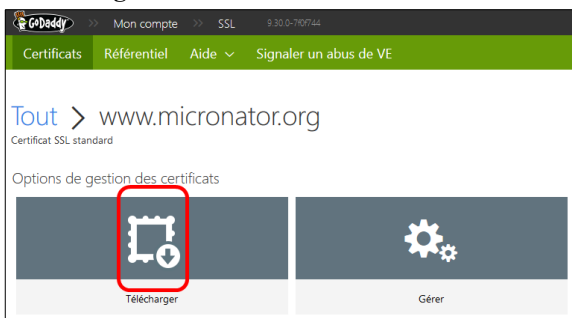
- On vérifie notre courriel (*adresse de courriel du gestionnaire du compte GoDaddy*).
- On clique sur le lien sous **Étape 1** pour télécharger le fichier zip.



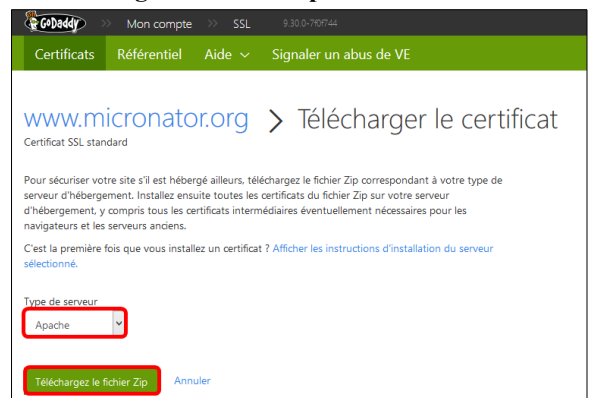
Chez **GoDaddy**, on clique **Afficher le statut**.



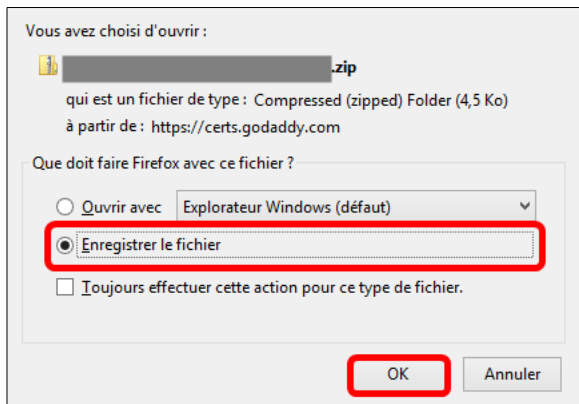
Télécharger.






- **Type de serveur Apache.**
- **Télécharger le fichier Zip.**



- Choisir le bouton **Enregistrer le fichier** | **OK**.



- On dézippe et 2 fichiers sont extraits.
- Le 1er fichier est le certificat.
- Le 2e fichier est celui de la chaîne de certification.

Nom	Modifié le	Type	Taille
 3ec...71.crt	2016-01-27 09:17	Certificat de sécur...	2 Ko
 gd_bundle-g2-g1.crt	2016-01-27 09:17	Certificat de sécur...	5 Ko
 yruo...@g.zip	2016-01-27 11:18	Dossier compressé	5 Ko

On est prêt à installer notre nouveau certificat.

VI- Installation

1. Introduction théorique

Référence SME:

http://wiki.contribs.org/Certificate_Integration_GoDaddy_Certificate.

1.1. Version du serveur web Apache pour SME-9.1

```
[root@dorgee ~]# rpm -qa | grep apache
e-smith-apache-2.4.0-12.el6.sme.noarch
[root@dorgee ~]#
```

Référence pour le tableau ci-dessous:

<https://ca.godaddy.com/fr/help/installation-dun-certificat-ssl-dans-apache-centos-5238>.

<i>Apache version < 2.4.8</i>		<i>Apache version 2.4.8+</i>	
Directive	Chemin à saisir	Directive	Chemin à saisir
SSLCertificateFile	Chemin du fichier du certificat	SSLCertificateFile	Chemin du fichier du certificat
SSLCertificateKeyFile	Chemin du fichier de clés	SSLCertificateKeyFile	Chemin du fichier de clés
SSLCertificateChainFile	Chemin du bundle intermédiaire	SSLCACertificatePath	Chemin du bundle intermédiaire

1.2. Module Apache mod_ssl

Référence: https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatekeyfile..

Description	Chiffrement de haut niveau basé sur les protocoles Secure Sockets Layer (SSL) et Transport Layer Security (TLS)
Statut	Extension
Identificateur de Module	ssl_module
Fichier Source	mod_ssl.c

1.2.1. Sommaire

Ce module fournit le support **SSL v3** et **TLS v1** au serveur **HTTP Apache**. **SSL v2** n'est plus supporté.

Ce module s'appuie sur [OpenSSL](#) pour fournir le moteur de chiffrement.

D'autres détails, discussions et exemples sont fournis dans la [documentation SSL](#).

1.3. Directive SSLCertificateFile

Description	Fichier de données contenant le certificat X.509 du serveur codé en PEM
Syntaxe	SSLCertificateFile chemin-fichier
Contexte	configuration du serveur, serveur virtuel
Statut	Extension
Module	mod_ssl

Cette directive permet de définir le fichier de données contenant les informations de certificat **X.509** du serveur codées au format **PEM**. Ce fichier doit contenir au minimum un certificat d'entité finale (*feuille*). La directive peut être utilisée plusieurs fois (*elle référence des fichiers différents*) pour accepter plusieurs algorithmes d'authentification au niveau du serveur - souvent RSA, DSA et ECC. Le nombre d'algorithmes supportés dépend de la version d'OpenSSL utilisée avec mod_ssl : à partir de la version 1.0.0, la commande **openssl list-public-key-algorithms** affiche la liste des algorithmes supportés.

Les fichiers peuvent aussi contenir des certificats de **CA** intermédiaires triés depuis la feuille vers la racine. Cette fonctionnalité est disponible depuis la version 2.4.8 du serveur HTTP Apache, et rend obsolète la directive **SSLCertificateChainFile**. A partir de la version 1.0.2 d'OpenSSL, il est alors possible de configurer la chaîne de certification en fonction du certificat.

Depuis la version 2.4.7 du serveur HTTP Apache, on peut aussi ajouter des paramètres DH personnalisés et un nom EC curve pour les clés éphémères à la fin du premier fichier défini par la directive SSLCertificateFile. Ces paramètres peuvent être générés avec les commandes openssl dhparam et openssl eparam, et ils peuvent être ajoutés tel quel à la fin du premier fichier de certificat. En effet, seul le premier fichier de certificat défini peut être utilisé pour enregistrer des paramètres personnalisés, car ces derniers s'appliquent indépendamment de l'algorithme d'authentification utilisé.

Enfin, il est aussi possible d'ajouter la clé privée du certificat de l'entité finale au fichier de certificat, ce qui permet de se passer d'une directive SSLCertificateKeyFile séparée. Cette pratique est cependant fortement déconseillée. En effet, les fichiers de certificats qui contiennent de tels clés embarquées doivent être définis avant les certificats en utilisant un fichier de clé séparé. En outre, si la clé est chiffrée, une boîte de dialogue pour entrer le mot de passe de la clé s'ouvre au démarrage du serveur.

1.3.1. Interopérabilité des paramètres DH avec les nombres premiers de plus de 1024 bits

Depuis la version 2.4.7, mod_ssl utilise des paramètres DH standardisés avec des nombres premiers de 2048, 3072 et 4096 bits, et avec des nombres premiers de 6144 et 8192 bits depuis la version 2.4.10 (voir RFC 3526), et les fournit aux clients en fonction de la longueur de la clé du certificat RSA/DSA. En particulier avec les clients basés sur Java (versions 7 et antérieures), ceci peut provoquer des erreurs au cours de la négociation - voir cette réponse de la FAQ SSL pour contourner les problèmes de ce genre.

1.3.2. Exemple pour SME

```
SSLCertificateFile /home/e-smith/ssl.crt/dorgee.micronator.org.crt
```

1.4. Directive SSLCertificateKeyFile

Description	Fichier contenant la clé privée du serveur codée en PEM
Syntaxe	SSLCertificateKeyFile chemin-fichier
Contexte	configuration du serveur, serveur virtuel
Statut	Extension
Module	mod_ssl

Cette directive permet de définir le fichier contenant la clé privée du serveur codée en **PEM**. Si la clé privée est chiffrée, une boîte de dialogue demandant le mot de passe s'ouvre au démarrage.

Cette directive peut être utilisée plusieurs fois pour référencer différents noms de fichiers, afin de supporter plusieurs algorithmes pour l'authentification du serveur. A chaque directive **SSLCertificateKeyFile** doit être associée une directive **SSLCertificateFile** correspondante.

La clé privée peut aussi être ajoutée au fichier défini par la directive **SSLCertificateFile**, mais cette pratique est fortement déconseillée. En effet, les fichiers de certificats qui comportent une telle clé doivent être définis après les certificats en utilisant un fichier de clé séparé.

1.4.1. Exemple pour SME

```
SSLCertificateKeyFile /home/e-smith/ssl.key/dorgee.micronator.org.key
```

1.5. Directive SSLCertificateChainFile

Description	Fichier contenant les certificats de CA du serveur codés en PEM
Syntaxe	SSLCertificateChainFile chemin-fichier
Contexte	configuration du serveur, serveur virtuel
Statut	Extension
Module	mod_ssl



SSLCertificateChainFile est obsolète

SSLCertificateChainFile est devenue obsolète avec la version 2.4.8, lorsque la directive **SSLCertificateFile** a été étendue pour supporter aussi les certificats de **CA** intermédiaires dans le fichier de certificats du serveur.

Cette directive permet de définir le fichier optionnel **tout-en-un** (*Bundle*) où vous pouvez rassembler les certificats des Autorités de Certification (**CA**) qui forment la chaîne de certification du certificat du serveur. Cette chaîne débute par le certificat de la **CA** qui a délivré le certificat du serveur et peut remonter jusqu'au certificat de la **CA** racine. Un tel fichier contient la simple concaténation des différents certificats de **CA** codés en **PEM**, en général dans l'ordre de la chaîne de certification.

Elle doit être utilisée à la place et/ou en complément de la directive **SSLCACertificatePath** pour construire explicitement la chaîne de certification du serveur qui est envoyée au navigateur en plus du certificat du serveur. Elle s'avère particulièrement utile pour éviter les conflits avec les certificats de **CA** lorsqu'on utilise l'authentification du client. Comme le fait de placer un certificat de **CA** de la chaîne de certification du serveur dans la directive **SSLCACertificatePath** produit le même effet pour la construction de la chaîne de certification, cette directive a pour effet collatéral de faire accepter les certificats clients fournis par cette même **CA**, au cours de l'authentification du client.

Soyez cependant prudent: fournir la chaîne de certification ne fonctionne que si vous utilisez un simple certificat de serveur **RSA** ou **DSA**. Si vous utilisez une paire de certificats couplés **RSA+DSA**, cela ne fonctionnera que si les deux certificats utilisent vraiment la même chaîne de certification. Dans le cas contraire, la confusion risque de s'installer au niveau des navigateurs.

1.5.1. Exemple pour SME

```
SSLCertificateChainFile /home/e-smith/ssl.crt/gd_bundle-g2-g1.crt
```

2. Création d'un répertoire de travail

On se logue au **Serveur SME-9.1** avec **PuTTY**.

On vérifie qu'on est bien dans le répertoire personnel de l'utilisateur **root**.

```
[root@dorgee ~]# pwd
/root
[root@dorgee ~]#
```

On crée un répertoire de travail qui conservera les fichiers originaux du certificat.

```
[root@dorgee ~]# mkdir GoDaddy
[root@dorgee ~]#
```

On sécurise le répertoire

```
[root@dorgee ~]# chmod 700 GoDaddy/
[root@dorgee ~]#
```

On vérifie.

```
[root@dorgee ~]# ls -alsd GoDaddy/
4 drwx----- 2 root root 4096 24 janv. 11:51 GoDaddy/
[root@dorgee ~]#
```

On se rend dans le répertoire de travail.

```
[root@dorgee ~]# cd GoDaddy/
[root@dorgee GoDaddy]#
```

On vérifie.

```
[root@dorgee GoDaddy]# pwd
/root/ GoDaddy
[root@dorgee GoDaddy]#
```

3. Emplacement des fichiers du certificat actuel

On recherche l'emplacement des fichiers originaux du certificat en lançant la commande ci-dessous.

```
[root@dorgee GoDaddy]# cat /etc/httpd/conf/httpd.conf | grep SSLCertificate
SSLCertificateFile /home/e-smith/ssl.crt/dorgee.micronator.org.crt
SSLCertificateKeyFile /home/e-smith/ssl.key/dorgee.micronator.org.key
[root@dorgee GoDaddy]#
```

On vérifie le chemin du certificat.

```
[root@dorgee GoDaddy]# ls -als /home/e-smith/ssl.crt/dorgee.micronator.org.crt
4 -rw-r--r-- 1 root root 1156 22 déc. 07:23 /home/e-smith/ssl.crt/dorgee.micronator.org.crt
[root@dorgee GoDaddy]#
```

On vérifie le chemin de la clé privée.

```
[root@dorjee GoDaddy]# ls -als /home/e-smith/ssl.key/dorjee.micronator.org.key
4 -rw-r--r-- 1 root root 888 19 mai 2007 /home/e-smith/ssl.key/dorjee.micronator.org.key
[root@dorjee GoDaddy]#
```

4. Sauvegarde des fichiers originaux

On crée un répertoire pour la sauvegarde les fichiers originaux.

```
[root@dorjee GoDaddy]# mkdir Originaux
[root@dorjee GoDaddy]#
```

On sécurise le répertoire

```
[root@dorjee GoDaddy]# chmod 700 Originaux/
[root@dorjee GoDaddy]#
```

On vérifie.

```
[root@dorjee GoDaddy]# ls -alsd Originaux/
4 drwx----- 2 root root 4096 25 janv. 05:40 Originaux/
[root@dorjee GoDaddy]#
```

On se rend dans le répertoire de sauvegarde.

```
[root@dorjee GoDaddy]# cd Originaux/
[root@dorjee Originaux]#
```

On vérifie.

```
[root@dorjee Originaux]# pwd
/root/GoDaddy/Originaux
[root@dorjee Originaux]#
```

4.1. La clé originale

```
[root@dorjee Originaux]# cp /home/e-smith/ssl.key/dorjee.micronator.org.key .
[root@dorjee Originaux]#
```

On vérifie.

```
[root@dorjee Originaux]# ls -als
total 12
4 drwxr-xr-x 2 root root 4096 25 janv. 05:44 .
4 drwx----- 3 root root 4096 25 janv. 05:40 ..
4 -rw-r--r-- 1 root root 1704 25 janv. 05:44 dorjee.micronator.org.key
[root@dorjee Originaux]#
```

4.2. Le certificat original

```
[root@dorgee Originaux]# cp /home/e-smith/ssl.crt/dorgee.micronator.org.crt .
[root@dorgee Originaux]#
```

On vérifie.

```
[root@dorgee Originaux]# ls -als
total 16
4 drwxr-xr-x 2 root root 4096 25 janv. 05:45 .
4 drwx----- 3 root root 4096 25 janv. 05:40 ..
4 -rw-r--r-- 1 root root 1883 25 janv. 05:45 dorgee.micronator.org.crt
4 -rw-r--r-- 1 root root 1704 25 janv. 05:44 dorgee.micronator.org.key
[root@dorgee Originaux]#
```

4.3. Le fichier pem original

```
[root@dorgee Originaux]# cp /home/e-smith/ssl.pem/dorgee.micronator.org.pem .
[root@dorgee Originaux]#
```

On vérifie.

```
[root@dorgee Originaux]# ls -als
total 28
4 drwxr-xr-x 2 root root 4096 25 janv. 05:56 .
4 drwx----- 3 root root 4096 25 janv. 05:40 ..
4 -rw-r--r-- 1 root root 1883 25 janv. 05:45 dorgee.micronator.org.crt
4 -rw-r--r-- 1 root root 1704 25 janv. 05:44 dorgee.micronator.org.key
12 -rw-r--r-- 1 root root 8763 25 janv. 05:56 dorgee.micronator.org.pem
[root@dorgee Originaux]#
```

4.4. Le fichier original de la chaîne de certification (*bundle*)

On sauvegarde le fichier de la chaîne de certification.

```
[root@dorgee Originaux]# cp /etc/pki/tls/certs/ca-bundle.crt .
[root@dorgee Originaux]#
```

On vérifie.

```
[root@dorgee Originaux]# ls -als
total 888
4 drwxr-xr-x 2 root root 4096 25 janv. 05:59 .
4 drwx----- 3 root root 4096 25 janv. 05:40 ..
860 -rw-r--r-- 1 root root 877042 25 janv. 05:59 ca-bundle.crt
4 -rw-r--r-- 1 root root 1883 25 janv. 05:45 dorgee.micronator.org.crt
4 -rw-r--r-- 1 root root 1704 25 janv. 05:44 dorgee.micronator.org.key
12 -rw-r--r-- 1 root root 8763 25 janv. 05:56 dorgee.micronator.org.pem
[root@dorgee Originaux]#
```



Il se pourrait fort bien qu'on ait pas de fichier de chaîne de certification. Celui-ci est ordinairement inclus avec le fichier ZIP, après une requête CSR à une CA.

5. Copie des nouveaux fichiers vers le répertoire de travail

On retourne dans le répertoire de travail.


```
[root@dorgée Originiaux]# cd ..
[root@dorgée GoDaddy]#
```

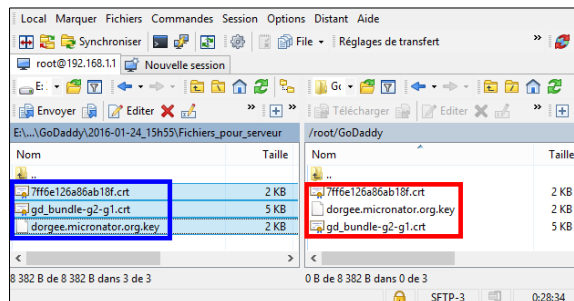
On vérifie.

```
[root@dorgée GoDaddy]# pwd
/root/GoDaddy
[root@dorgée GoDaddy]#
```

On copie tous les fichiers relatifs au nouveau certificat dans le répertoire de travail à l'aide de WinSCP ou de FileZilla.

Le répertoire de travail est: /root/GoDaddy.

 Il faut remplacer le nom des fichiers par **le nom de vos propres fichiers SSL**.



On vérifie la copie des fichiers.

```
[root@dorgée GoDaddy]# ls -als
total 28
4 drwx----- 3 root root 4096 25 janv. 06:06 .
4 drwxr-x--- 16 root root 4096 24 janv. 14:02 ..
4 -rw-r--r-- 1 root root 1883 24 janv. 14:13 7ff6e126a86ab18f.crt
4 -rw-r--r-- 1 root root 1704 23 janv. 10:08 dorgée.micronator.org.key
8 -rw-r--r-- 1 root root 4795 24 janv. 14:13 gd_bundle-g2-g1.crt
4 drwxr----- 2 root root 4096 25 janv. 05:59 Originiaux
[root@dorgée GoDaddy]#
```

6. Installation des fichiers du nouveau certificat

6.1. Certificat GoDaddy

Copier en renommant le fichier du certificat GoDaddy vers son répertoire final



```
[root@dorgée GoDaddy]# cp 7ff6e126a86ab18f.crt \
/home/e-smith/ssl.crt/dorgée.micronator.org.crt
cp : voulez-vous écraser « /home/e-smith/ssl.crt/dorgée.micronator.org.crt » ? y
[root@dorgée GoDaddy]#
```

On vérifie.

```
[root@dorgée GoDaddy]# ls -als /home/e-smith/ssl.crt/
total 12
4 drwx----- 2 root root 4096 25 janv. 06:10 .
4 drwxr-xr-x 10 admin admin 4096 24 janv. 12:14 ..
4 -rw-r--r-- 1 root root 1883 25 janv. 06:10 dorgée.micronator.org.crt
[root@dorgée GoDaddy]#
```

6.2. Clé privée du serveur SME



Nous avons généré cette clé privée lors de la création de la requête CSR. Elle devient la nouvelle clé privée du **Serveur SME-9.1**.

Copier le fichier de la nouvelle clé privée vers son répertoire final.



```
[root@dorgee GoDaddy]# cp dorgee.micronator.org.key \
/home/e-smith/ssl.key/dorgee.micronator.org.key

cp : voulez-vous écraser « /home/e-smith/ssl.key/dorgee.micronator.org.key » ? Y
[root@dorgee GoDaddy]#
```

On vérifie.

```
[root@dorgee GoDaddy]# ls -als /home/e-smith/ssl.key/dorgee.micronator.org.key

4 -rw-r--r-- 1 root root 1704 25 janv. 06:12 /home/e-smith/ssl.key/dorgee.micronator.org.key
[root@dorgee GoDaddy]#
```

6.3. Chaîne de certification (*bundle*)

On doit maintenant ajouter la chaîne de certification ("*bundle*").

On copie le fichier **bundle** vers le répertoire des certificats.

```
[root@dorgee GoDaddy]# cp gd_bundle-g2-g1.crt /home/e-smith/ssl.crt/

[root@dorgee GoDaddy]#
```

On vérifie.

```
[root@dorgee GoDaddy]# ls -als /home/e-smith/ssl.crt/

total 20
4 drwx----- 2 root root 4096 25 janv. 06:13 .
4 drwxr-xr-x 10 admin admin 4096 24 janv. 12:14 ..
4 -rw-r--r-- 1 root root 1883 25 janv. 06:10 dorgee.micronator.org.crt
8 -rw-r--r-- 1 root root 4795 25 janv. 06:13 gd_bundle-g2-g1.crt
[root@dorgee GoDaddy]#
```

6.4. Effaçage de l'ancien fichier pem

À la fin du prochain paragraphe, lors de la signalisation, un nouveau fichier **pem** va être recréé.

```
[root@dorgee GoDaddy]# rm /home/e-smith/ssl.pem/dorgee.micronator.org.pem

rm : supprimer fichier « /home/e-smith/ssl.pem/dorgee.micronator.org.pem » ? Y
[root@dorgee GoDaddy]#
```

On vérifie.

```
[root@dorgee GoDaddy]# ls -als /home/e-smith/ssl.pem/

total 8
4 drwx----- 2 root root 4096 25 janv. 06:42 .
4 drwxr-xr-x 10 admin admin 4096 24 janv. 10:49 ..
[root@dorgee GoDaddy]#
```

6.5. Mise à jour de la configuration de la BD de SME

Certificat.

```
[root@dorjee GoDaddy]# config setprop modSSL \
    crt /home/e-smith/ssl.crt/dorjee.micronator.org.crt
[root@dorjee GoDaddy]#
```

Clé privée.

```
[root@dorjee GoDaddy]# config setprop modSSL \
    key /home/e-smith/ssl.key/dorjee.micronator.org.key
[root@dorjee GoDaddy]#
```

Chaîne de certification.

```
[root@dorjee GoDaddy]# config setprop modSSL \
    CertificateChainFile \
    /home/e-smith/ssl.crt/gd_bundle-g2-g1.crt
[root@dorjee GoDaddy]#
```

On ajoute le **Nom Commun** à la base de données de SME.


```
[root@dorjee GoDaddy]# config setprop modSSL CommonName www.micronator.org
[root@dorjee GoDaddy]#
```

Vérification

```
[root@dorjee GoDaddy]# config show modSSL
modSSL=service
CertificateChainFile=/home/e-smith/ssl.crt/gd_bundle-g2-g1.crt
CommonName=www.micronator.org
TCPPort=443
access=public
crt=/home/e-smith/ssl.crt/dorjee.micronator.org.crt
key=/home/e-smith/ssl.key/dorjee.micronator.org.key
status=enabled
[root@dorjee GoDaddy]#
```

6.6. Application des changements

Si on ne veut pas réamorcer, on lance les commandes suivantes.

 (Peut prendre quelques secondes.)

```
[root@dorjee GoDaddy]# signal-event domain-modify ; signal-event email-update
[root@dorjee GoDaddy]#
```

Si on veut réamorcer, on applique les changements en signalant une mise à jour et un réamorçage.

```
[root@dorjee GoDaddy]# signal-event post-upgrade ; signal-event reboot
[root@dorjee GoDaddy]#
```

6.7. Vérification de la création du fichier pem

Après la signalisation ou le réamorçage, on affiche la date actuelle.

```
[root@dorgee GoDaddy]# date  
lun. janv. 25 06:23:06 EST 2016  
[root@dorgee GoDaddy]#
```

On affiche la date de création du fichier pem.

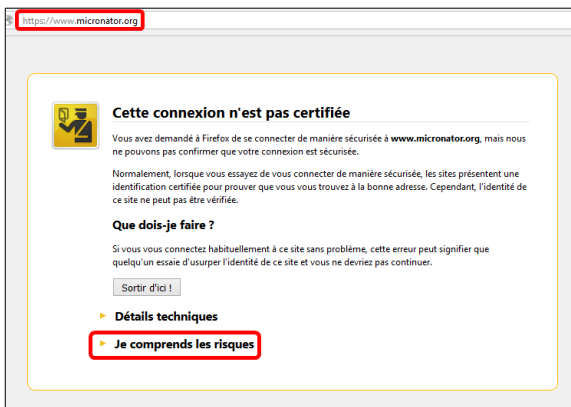
```
[root@dorgee GoDaddy]# ls -als /home/e-smith/ssl.pem/dorgee.micronator.org.pem  
12 -rw-r--r-- 1 root root 8763 25 janv. 06:21 /home/e-smith/ssl.pem/dorgee.micronator.org.pem  
[root@dorgee GoDaddy]#
```

Le fichier pem vient tout juste d'être recréé et le certificat est installé et fonctionnel.

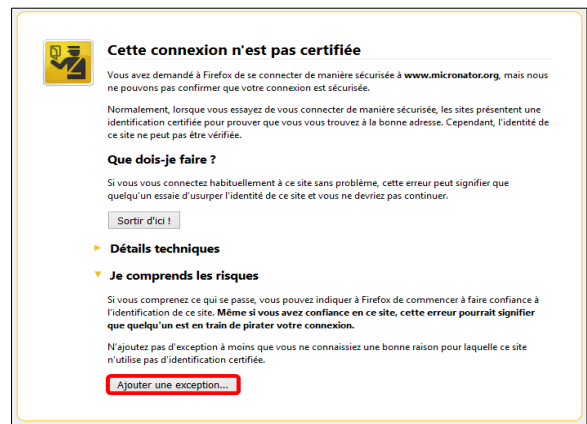
VII- Vérification

1. Vérification avec Firefox

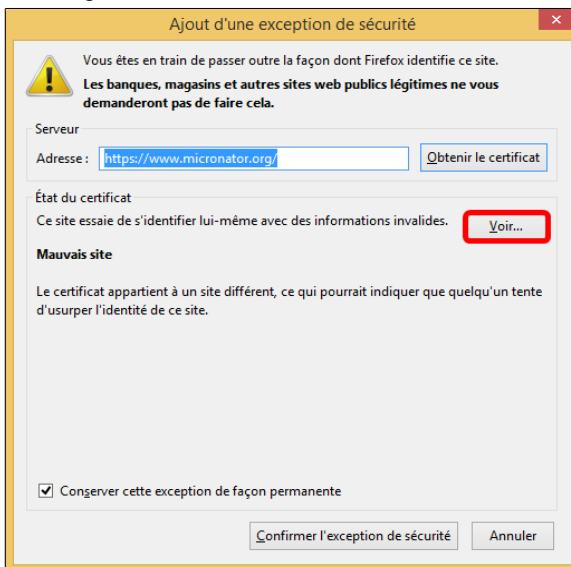
- On se rend à <https://www.micronator.org>.
- Je comprends les risques.



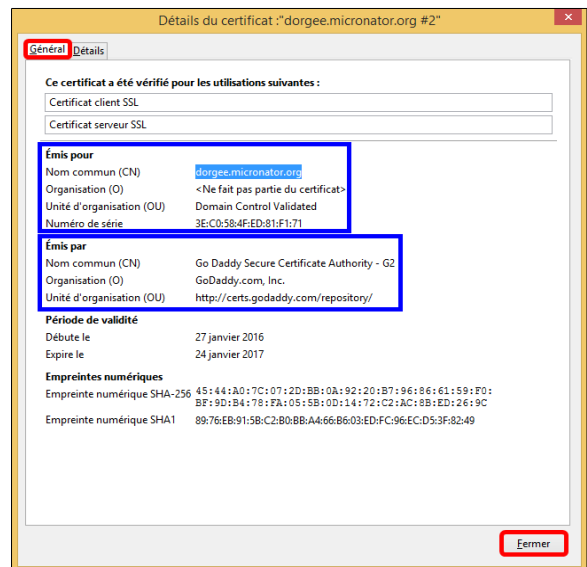
Ajouter une exception...



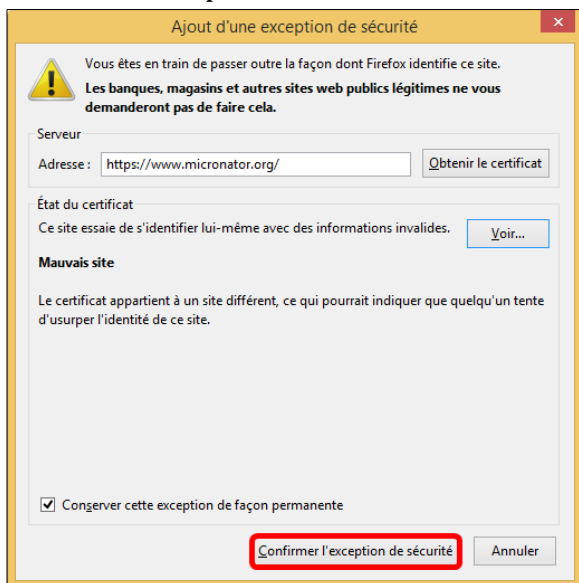
Voir... pour afficher les informations du certificat.



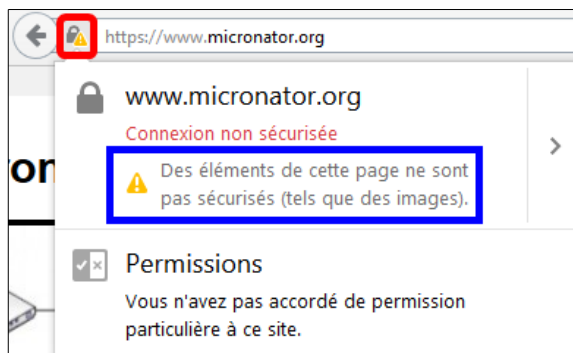
- Les informations du **certificat** sont affichées.
- Il s'agit bien de notre nouveau certificat.
- Fermer.



Confirmer l'exception de sécurité.

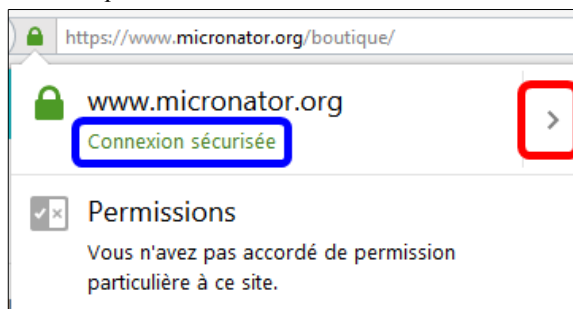


Au retour, on clique le petit cadenas pour afficher la mise en garde. Certains éléments ne sont pas sécurisés.



- Nous allons maintenant à la boutique à : <https://www.micronator.org/boutique>.
- On clique le cadenas.

- On voit que tout est sécurisé car le cadenas est vert.
- On clique l'icône > à droite.



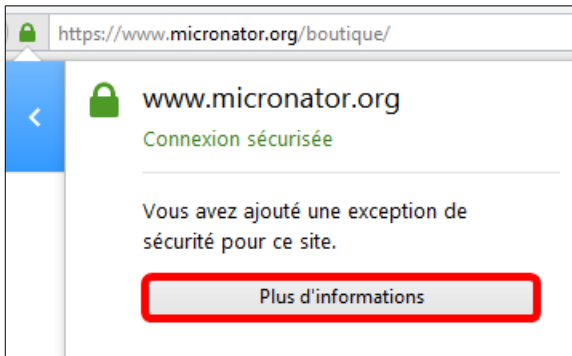
Le site de la boutique est dans un sous-répertoire du site principal et il a sa propre installation **WordPress**.

Dans le site **WordPress** de la boutique, nous avons ajouté l'extension **WordPress HTTPS** qui est destinée à être une solution tout-en-un pour l'utilisation de **SSL** sur les sites **WordPress**. Cette extension oblige toutes les pages à utiliser **https** et ainsi tout leur contenu est sécurisé.

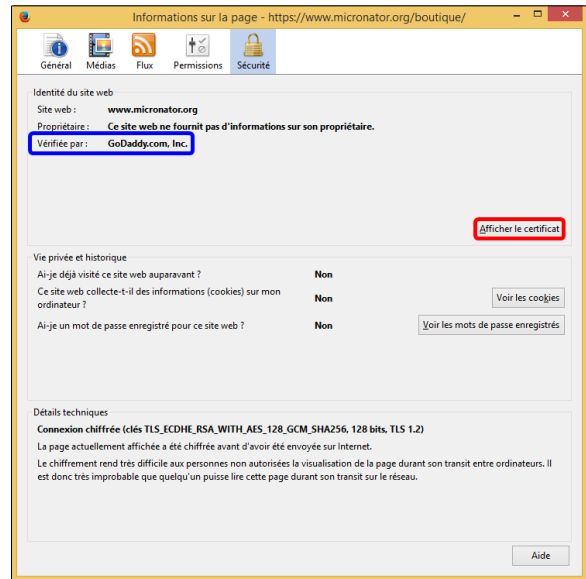
Cette extension n'est pas installée dans le **WordPress** du site principal.

Vérification

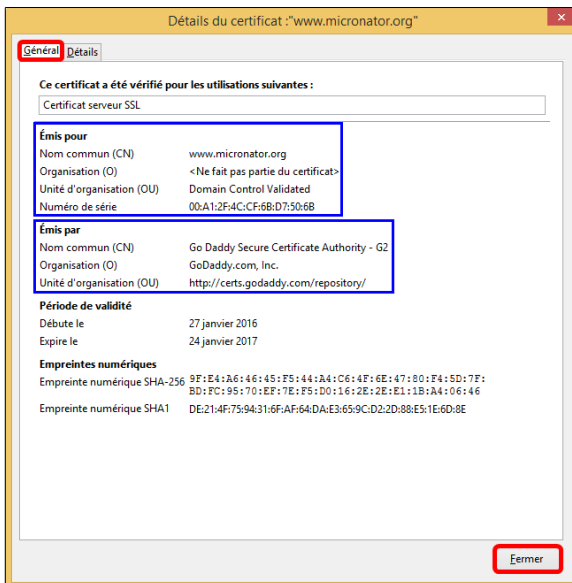
Plus d'informations.



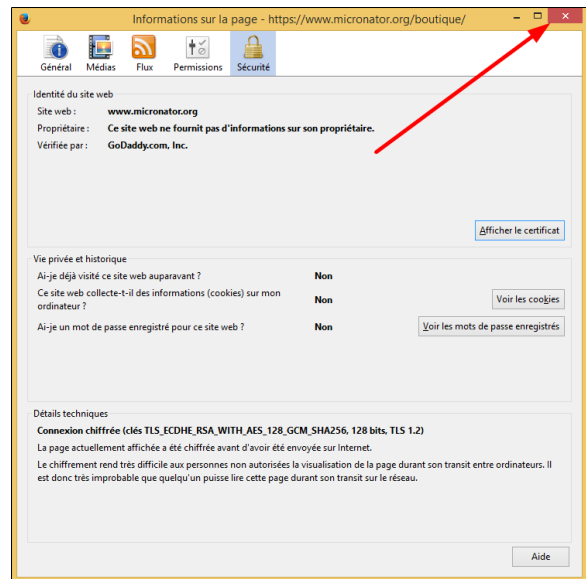
- Le site est vérifié par **GoDaddy.com. Inc.**
- **Afficher le certificat.**



- On peut voir pour qui le certificat a été émis: **www.micronator.org** et par qui: **GoDaddy Secure Certificate Authority - G2**.
- **Fermer.**

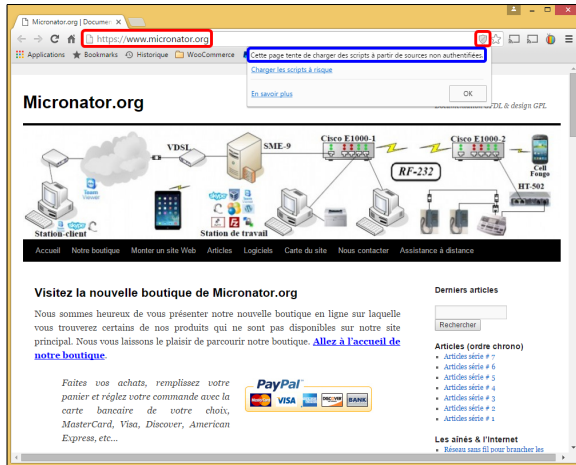


Au retour, on ferme avec le **X**, à droite en haut.



2. Vérification avec Google Chrome

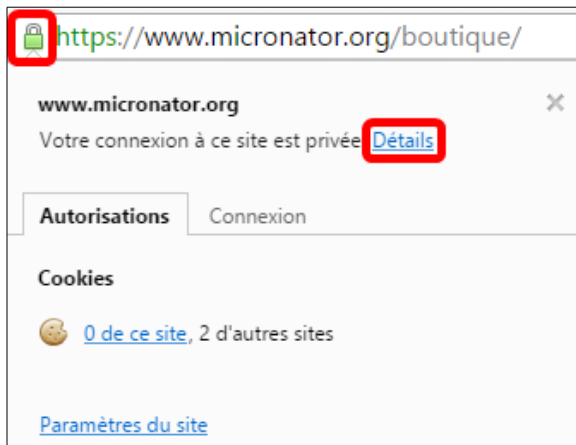
Sur le site principal, on clique l'icône du petit écu à droite et Google Chrome donne la même raison que Firefox.



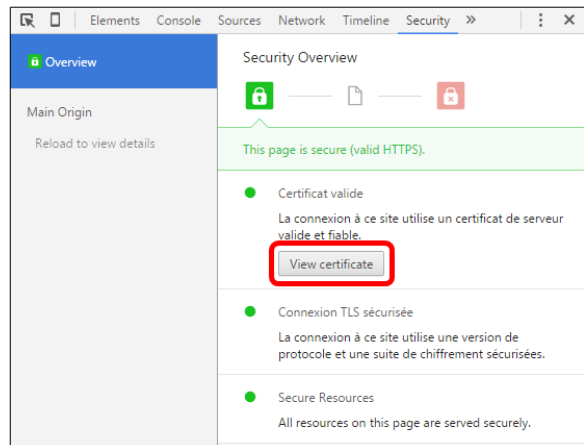
Sur le site de la boutique, Google Chrome a la même réaction que Firefox: petit cadenas vert, tout est sécurisé.



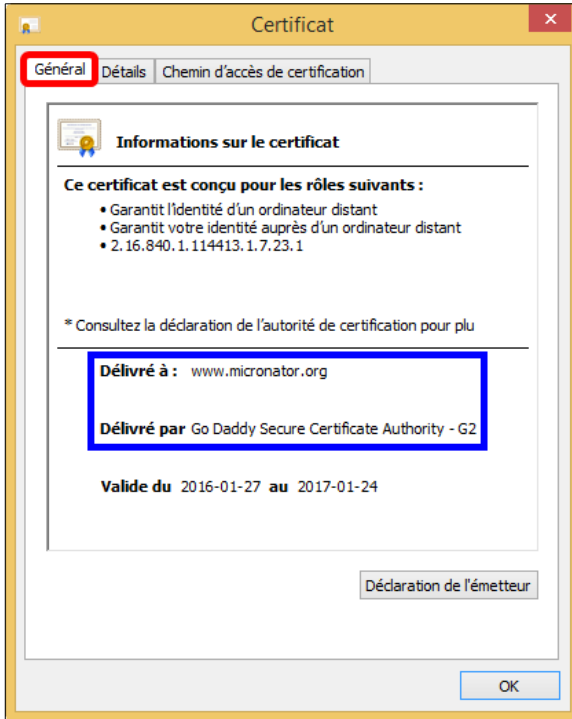
- On clique le petit cadenas.
- Détails.



- Le certificat est valide, la connexion TLS est sécurisée de même que les ressources.
- View certificate.

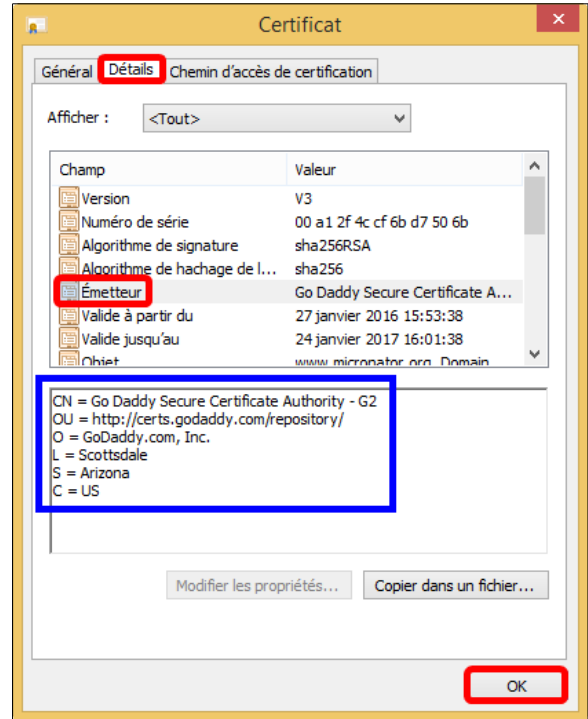


Onglet Général, même informations que Firefox.



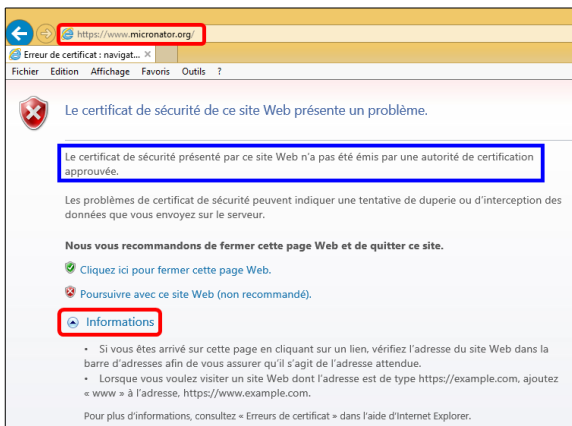
- Onglet Détails | Émetteur et on voit toute les informations de GoDaddy.

- Ok | OK | X pour tout fermer.

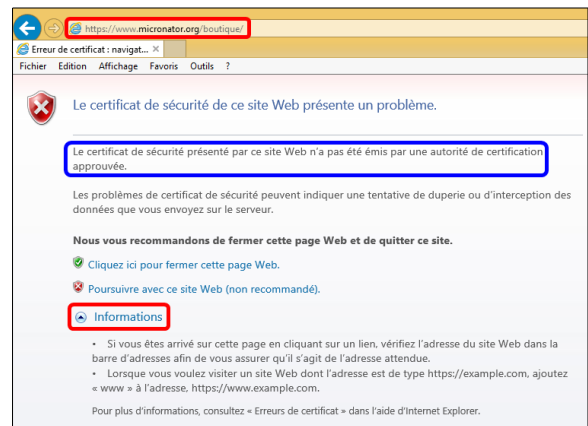


3. Vérification avec l'Explorateur Internet de Microsoft

Sur le site principal, EI affiche que le certificat n'a pas été émis par une autorité approuvée.



Sur le site de la boutique, EI affiche que le certificat n'a pas été émis par une autorité approuvée.



Les résultats qu'on voit ici sont dûs au module de l'antivirus **Avast** pour **EI**. Ce module est un genre d'homme-entre-les-deux (*man in the middle*) qui intercepte toutes les requêtes **https** et émet son propre certificat. Vue que **Avast** n'est pas une **CA** approuvée, **EI** émet une erreur disant que le certificat n'a pas été émis par une autorité approuvée.

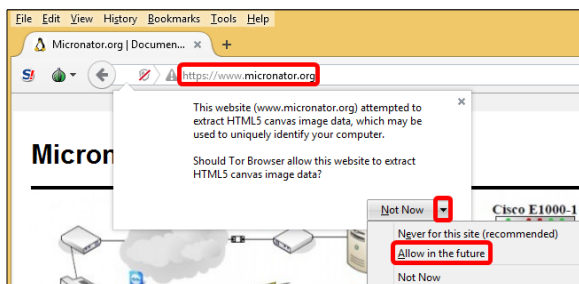
Même si on importe le fichier du certificat de **GoDaddy** dans **EI**, celui-ci persiste à utiliser celui de **Avast**.

Vu que chez **Micronator**, il est formellement interdit d'utiliser un navigateur **Microsoft** de quelle que version que ce soit, on n'insiste pas.

4. Vérification avec le navigateur TOR

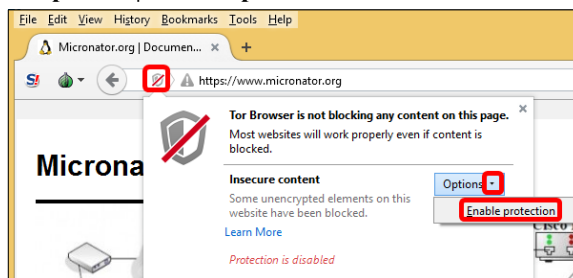
- Sur le site principal, Tor n'aime pas notre analyseur de log web.

- **Allow in the future.**



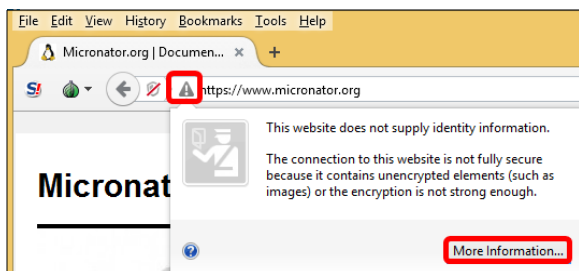
- On clique le petit écu.

- **Options | Enable protection.**

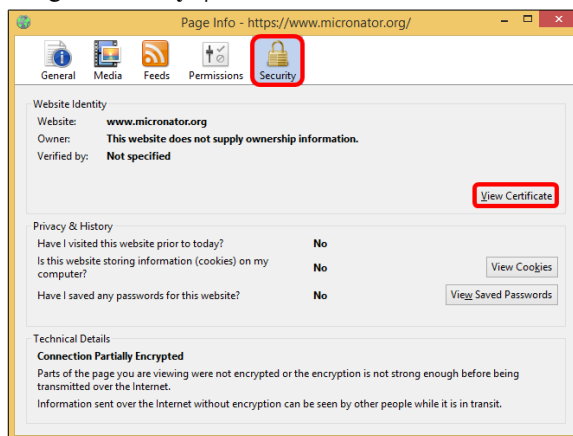


- On clique le triangle.

- **More information.**

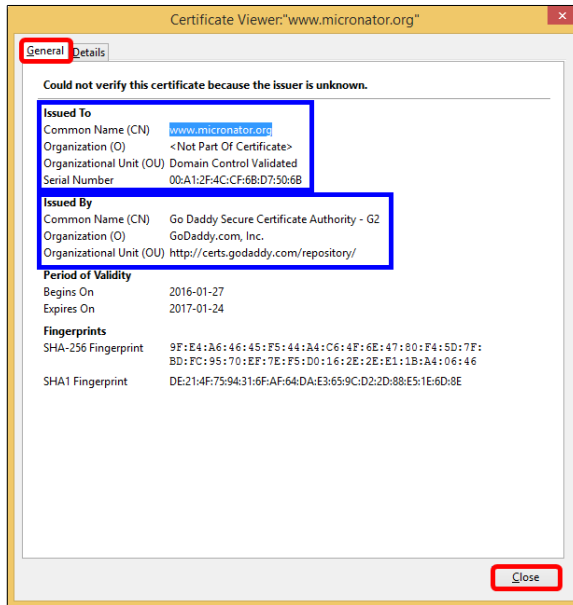


Onglet Security | View Certificate.

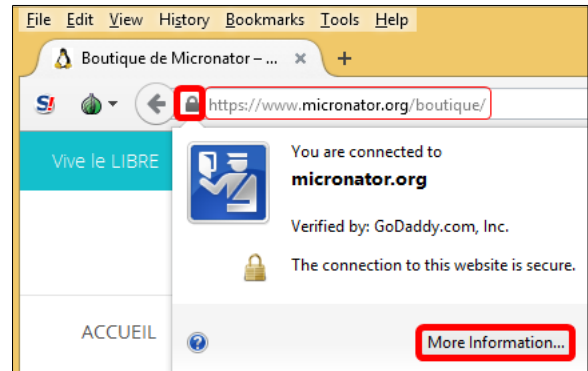


Vérification

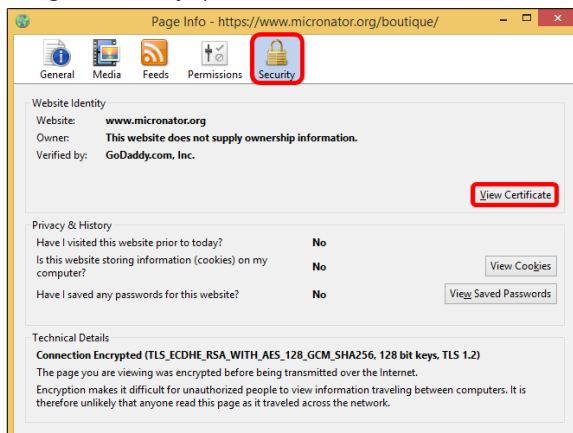
Dans l'onglet **General** on voit les mêmes informations qu'avec Firefox | **Close** | **X** pour tout fermer.



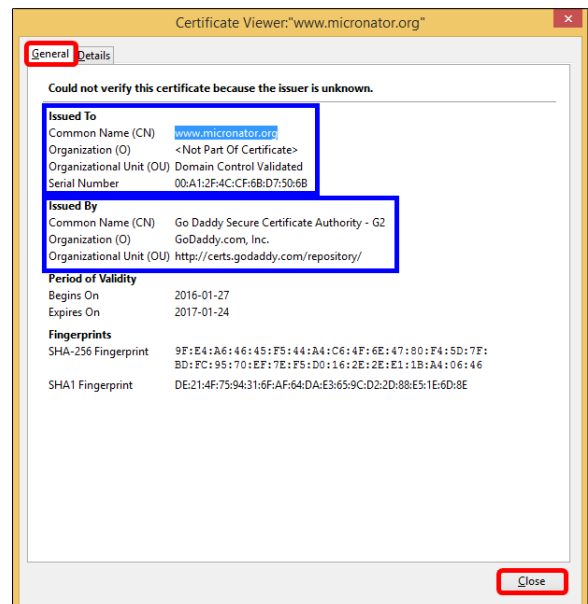
À la boutique, le cadenas sombre indique que le site ne fournit pas d'informations sur son propriétaire mais que la connexion est sécurisée. | **More Informations...**



Onglet **Security** | **View Certificate**.



Dans l'onglet **General** on voit les mêmes informations qu'avec Firefox | **Close** | **X** pour tout fermer.



5. Sceau de sécurité



5.1. Copie du code pour le sceau de sécurité GoDaddy

On retourne chez **GoDaddy**, on se rend dans la page du certificat.

À droite, on clique **Afficher le statut**.



- **Langue Français.**

- On sélectionne tout à l'intérieur du cadre du code avec [CTL] + [c].

Tout > www.micronator.org
Certificat SSL standard

Options de gestion des certificats

Télécharger Gérer

Détails du certificat

Statut	Certificat émis (Révoquer)
Nom de domaine	www.micronator.org
Puissance du cryptage	GoDaddy SHA-2
Période de validité	2016-1-27 - 2017-1-24
Numéro de série	a12f4ccf5bd7506b

Affichez le sceau de sécurité de votre certificat SSL

Créez votre sceau, copiez le code et collez-le dans le bas de page de votre site.

Couleur
Léger

Langue
Français

Aperçu

Code

```
<script id="stseal" type="text/javascript" src="https://www.godaddy.com/getSeal?sealID=AA44qChY7qz3O2BkVWjRl" data-bbox="768 448 871 478"></script>
```

Ctrl + pour copier

⚠ On colle le code dans un fichier texte tel que **NotePad++** ou **Bloc-notes**.

5.2. Installation du code dans le Pied de page du thème

On se connecte sur notre site **WordPress** qui devrait rouler notre **Thème enfant**.

Pour le **Thème enfant**, voir:

http://www.micronator.org/?page_id=2369.

On se rend dans le **Pied de page du thème** en cliquant **Tableau de bord** | **Apparence** | **Éditeur** | **Store WP Enfant** | **Pied de page du thème**.

Store WP Enfant Sélectionner

Modèles

Ce thème enfant hérite de certains modèles de son thème parent, [Store WP](#).

Pied de page du thème (footer.php)

Fonctions du thème (functions.php)

Styles

Feuille de style (style.css)

Vérification

À la fin du fichier **Pied de page du thème**, avant `</body>`, on colle le code (*en rouge*) qu'on a copié du site de **GoDaddy**. Avant et après ce code on entre les balises pour en faire un paragraphe centré (*en bleu*). Avant et après les balises du paragraphe, on insère les balises de division (*en magenta*). On peut ajouter une ligne vide (*en vert*).

Votre `sealID=jM4Wq...` va être différent de celui indiqué ci-dessous.

```

        <span style="font-family: georgia,palatino,serif; font-size:
10pt;">Conditions de vente</span>
    </span>
    </em>
    </a>
    </em>
</div><!-- .col7 -->
</br>
<div>
    <p style="text-align: center;">
        <span id="sitesead"><script type="text/javascript"
src="https://seal.godaddy.com/getSeal?
sealID=jM4WqOHYXtp2OZbkWeJ9imXZqEtX0Y5Fe1VXVCv61qcHZPHssNmnfEyK6v3a">
        </script>
        </span>
    </p>
</div>
</body>
</html>
```

On met le fichier à jour en cliquant **Mettre à jour le fichier**.



Si **Mettre à jour le fichier** n'apparaît pas, c'est que vous n'avez pas le droit d'écriture (`w`) sur le fichier: `/wp-content/themes/store-wp-enfant/footer.php`. Vous devez alors vous rendre dans le répertoire et lancer la commande suivante:

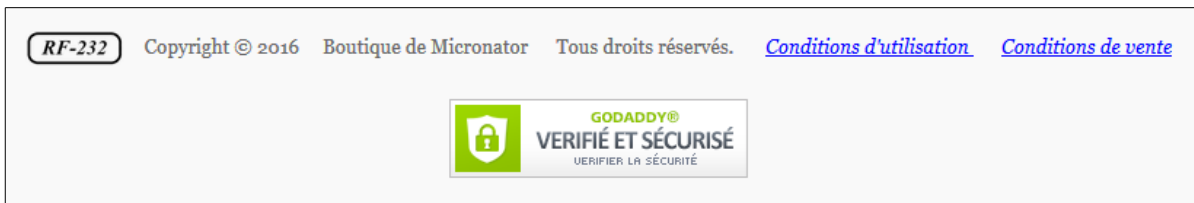


```
[root@dorgee store-wp-enfant]# chmod ug+w footer.php
[root@dorgee store-wp-enfant]#
```

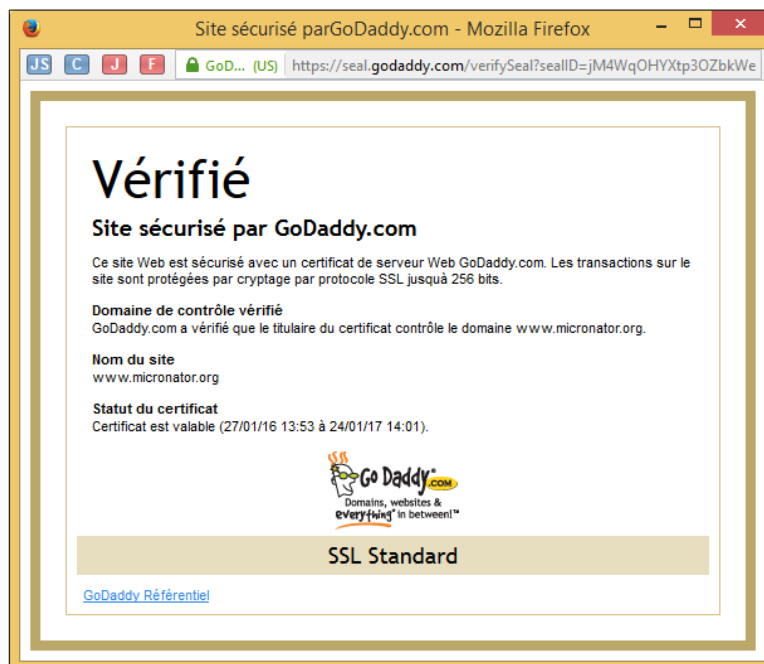
On vérifie.

```
[root@dorgee store-wp-enfant]# ls -asld footer.php
4 -rw-rw---- 1 admin shared 2509 27 janv. 11:34 footer.php
[root@dorgee store-wp-enfant]#
```

On se rend sur le site et on voit, dans le bas de la page, le sceau de sécurité **GoDaddy**. On clique sur celui-ci.



Vous verrez alors s'afficher la fenêtre ci-dessous.



VIII- Demander une certification à Namecheap

1. Introduction

Un autre endroit pour demander un certificat est **namecheap.com**.

Nous avons choisi **namecheap.com** pour notre requête **CSR** car son coût pour un certificat est de seulement \$9.00USD/\$13.46CAD (valeur du CAD en date du 17 janvier 2016).

C\$13.07 /yr <input type="text" value="1 year"/> Add to Cart	COMODO PositiveSSL Creating Trust Online PositiveSSL is one of the most popular and inexpensive SSL certificates in the industry. This hassle-free certificate is the ideal choice for websites where the brand's trust is already established and organization verification is not needed. It's ideal for securing low-volume e-commerce websites.	Single Domain
		\$10,000 Warranty
		15-Day Refund
		No Paperwork
		Learn More

Référence:

<http://www.ficgs.com/avis-forum-statistiques/cheap-domain-name-registration/namecheap.com>

Analyse : Ce site a pour hébergeur Global Net Access, LLC, il a 4,590 pages dans l'index de Google, il a pour content-type TEXT/HTML; CHARSET=WINDOWS-1252, il est placé sous la responsabilité de son auteur, Namecheap Domain Registration, SSL and Web Hosting, il a un Google PageRank de 6, il a pour attribut meta-tag de langage 'en' (anglais), il a pour location ATLANTA, GEORGIA, 30310, UNITED STATES, latitude: 33.7257003784 , longitude: -84.4309005737, ils server platform is Microsoft-IIS/7.0, il a 0 sous-domaines, il a été estimé selon un algorithme à une valeur de 2 Million (dollars), il a pour meta-tag robots INDEX, FOLLOW, ALL, il a 45,300 sites similaires selon Bing, il a 512 liens entrants selon Google (signifiant que namecheap.com est un site important), il a les mots-clés suivants dans ses meta-tags: "cheap domain names, domain names(4x), domains(18x), registration(24x), domain name registration(2x), web name registration, reserve webname, domain registration(3x), register url, free url forwarding, email forwarding, dns hosting, domain snapback, domian, registartion, cheap domains, ssl certificates, free ssl, freessl, domain transfer, domain renewal, , " pour un total de 23 mots-clés (probablement trop nombreux), il a un nombre de consultations de pages d'environ 1047619 par jour, il a un trafic rank Alexa de 1050, il a pour adresse IP de serveur 74.81.78.44, il a un revenu publicitaire quotidien potentiel estimé à environ 3599 dollars, il a 27100 liens entrants selon le moteur de recherche de Yahoo, ils web technology is ASP.NET, finalement il a 0 liens entrants selon Technorati.

2. Choix du certificat & création d'un compte

On se rend à l'adresse: <https://www.namecheap.com/security/ssl-certificates/domain-validation.aspx>

Add to Cart.

C\$13.07 /yr

COMODO PositiveSSL

PositiveSSL is one of the most popular and inexpensive SSL certificates in the industry. This hassle-free certificate is the ideal choice for websites where the brand's trust is already established and organization verification is not needed. It's ideal for securing low-volume e-commerce websites.

1 year

Add to Cart

Confirm Order.

Edit Cart

PositiveSSL 1 Year C\$13.07

Confirm Order

On entre les informations demandées. On lit les **Terms of Services** et si on est d'accord avec ceux-ci, on clique: **Create account and continue.**

Create An Account LOG IN?

New to Namecheap? Quickly signup for an account now.

Username michelandre

Password

Confirm Password

First Name

Last Name

Email Address

Yes, sign me up for Namecheap's newsletter

By creating an account, you agree with our [Terms of Service](#).

Create Account and Continue

On entre les informations demandées | **Continue.**

Account Contact Information

First Name

Last Name

I'm registering on behalf of a company

Address Line 1

Address Line 2

City

State/Province

Zip/Postal Code

Country Canada

Phone Number +1

Add phone extension

Fax Number +1 Fax Number OPTIONAL

Email Address

Account Security

Two-Factor Authentication adds a second layer of security to your account by requiring phone verification as well as a password. [Learn more](#)

Enable Two-Factor Authentication

Continue

Confirm Order.

Edit Cart

PositiveSSL 1 Year C\$13.07

Confirm Order

3. Paiement

- On choisit le mode de paiement.
- On vérifie les données de l'adresse etc...
- **Continue.**

Payment Method

Secure Card Payment

Paypal

We welcome your Paypal payment. Your Paypal account will not be charged until after you've confirmed your order.

Account Funds

Receipt Details

We'll provide your receipt. Please confirm the address.

Billing Address

Use default account contact

save the configuration above to my default payment settings

We'll save this information for future use.

Continue

On entre les informations demandées | **Submit.**

Enter above text

649

Submit

- On vérifie les informations.
- On clique l'**icône PayPal.**

We used your previously entered settings to select a payment method. If that's okay with you, simply continue reviewing your order. To change, select this option: [Review payment settings](#)

View Edit Order Details

Order Review

PositiveSSL 1 year \$9.00

Subtotal \$9.00 = C\$13.07

Payment Details

Payment Method PAYPAL

Issue Receipt for

PayPal

Your Subtotal \$9.00

Checkout PayPal

Select other payment options

Chez **PayPal**, on entre les informations demandées pour le paiement | **Connexion.**

namecheap

PayPal 9,00 \$ USD

Payer avec PayPal Français

En tant qu'utilisateur, vos achats admissibles sont couverts par la [Protection des Achats PayPal](#).

PayPal est le réflexe sécurité pour effectuer des paiements.

Peu importe où vous magasinez, nous protégeons vos informations financières.

Restez connecté pour payer plus rapidement

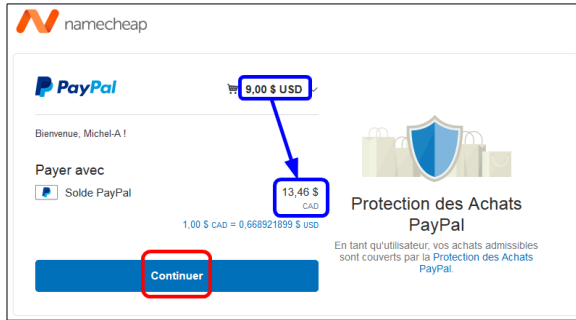
Connexion

Adresse de courriel ou mot de passe oublié ?

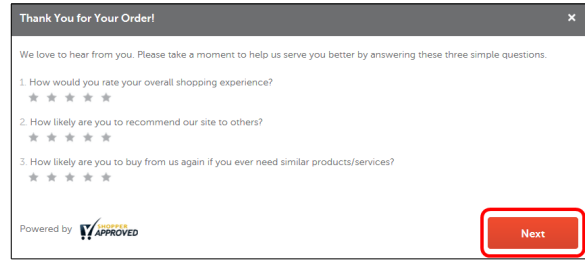
OU

Ouvrir un compte

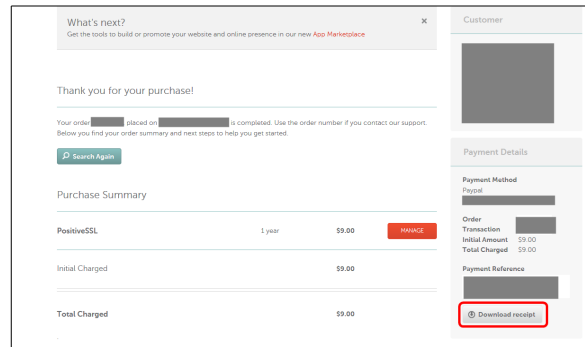
On vérifie | Continuer.



Next.

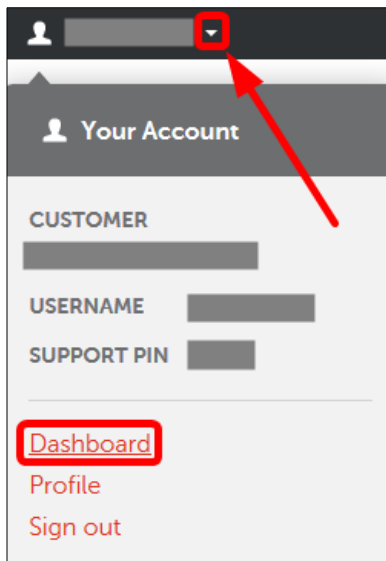


On peut télécharger un reçu de la transaction.

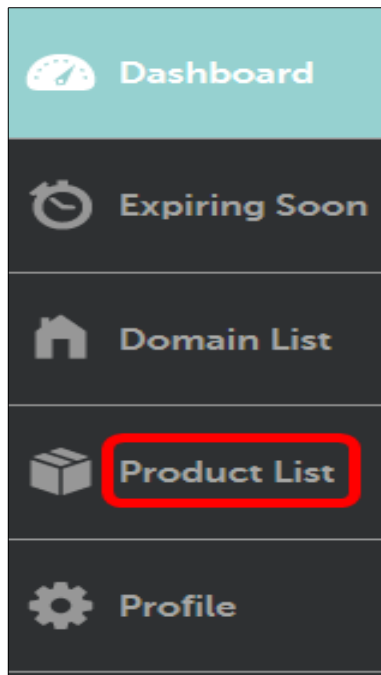


4. Activation du certificat

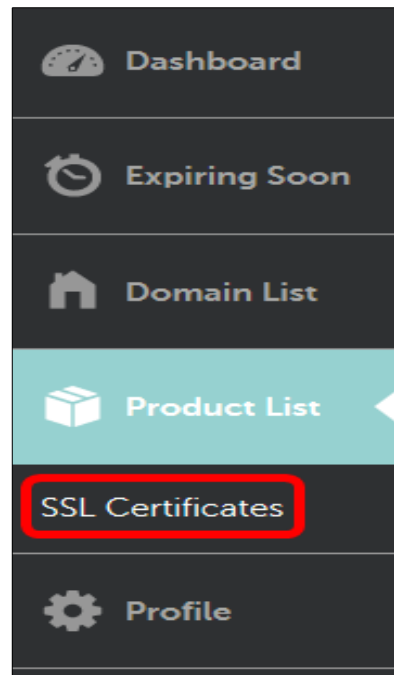
Sur le site namecheap.com, en haut à gauche, on clique la petite flèche gauche, pour dérouler le menu | Dashboard.



Product List.



SSL Certificates.



Demander une certification à Namecheap

ACTIVATE.

5. Copie du contenu de la requête



Pour **namecheap.com**, on utilise le répertoire de travail: **/root/CSR** pour créer la requête.



La requête CSR pour **namecheap.com** est générée de la même manière que pour **GoDaddy**. Voir le chapitre [Création de la requête CSR](#) à la page 9. On peut aussi utiliser la même requête utilisée par **GoDaddy**.

On se logue à notre serveur avec **PuTTY** pour pouvoir copier le contenu du fichier de notre requête CSR.

On se rend dans le répertoire dans lequel on a généré notre requête.

```
[root@dorgee ~]# cd CSR
[root@dorgee CSR]#
```

On vérifie.

```
[root@dorgee CSR]# pwd
/root/CSR
[root@dorgee CSR]#
```

On affiche liste nos fichiers.

```
[root@dorgee CSR]# ls -als
total 16
4 drwxr-xr-x 2 root root 4096 18 janv. 17:05 .
4 dr-xr-x--- 7 root root 4096 18 janv. 16:54 ..
4 -rw-r--r-- 1 root root 1074 18 janv. 17:05 dorgee.micronator.org.csr
4 -rw-r--r-- 1 root root 1704 18 janv. 17:05 dorgee.micronator.org.key
[root@dorgee CSR]#
```

On affiche le fichier de notre requête.

```
[root@dorgee CSR]# cat micronator.org.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC4TCCAckCAQAwZSxuCzAJBgNVBAYTAkNBAAswCQYDVQQIDAJRQzERMA8GA1EU
BwwITW9udHJlYWwDZANBgNVBAoMB1JGLTIzMjETMBEGA1UECwwKTWljcm9uYXVz
...
...
VU2Y0hPGj3LUUP8pJTXWdwCEzid4UHFN7stJ60vjcXre/beDEmocwdbsydXAcRc6
kIgZ4Y1SoPS2CA1MNxTmibfdDlnHw+hXjFYCs+ocVmh4ysqMTrXpFKiW1GpFZHST
tfnfa137mm2VpZIW86pj5ICg/JWq
-----END CERTIFICATE REQUEST-----

[root@dorgee CSR]#
```



On sélectionne tout entre **BEGIN** et **END**, on copie (avec **[CTL] + [c]**) incluant les lignes entières **BEGIN** et **END**. Il ne faut pas de lignes vides avant ou après **BEGIN** et **END**.

On retourne chez **namecheap.com** et on y colle ce qu'on vient de copier de notre fichier.

Product List → SSL Certificates → Activate

Activate PositiveSSL Certificate

1 CSR 2 Validation 3 Contacts 4 Confirm

Your CSR – or “Certificate Signing Request” – is base64 encoded data that contains a public key and information about the certificate applicant, such as organization, locality, state, country, and domain name for which the certificate should be issued. Usually, the CSR is generated server-side, along with the private key. Your CSR is required for activation of your SSL certificate. If you’re renewing an existing SSL certificate, you may use your previous CSR. However, that may create a security threat, so we recommend you get a new CSR every time. [Learn how to generate a CSR →](#)

Enter CSR

Primary Domain

Server Type

Hashing Algorithm

- On clique à l'extérieur du champ de la clé et le nom de notre domaine apparaît.
- **Server Type** on sélectionne **Apache, Nginx, Cpanel or other.**
- **Submit.**

Reissue PositiveSSL Certificate

1 CSR 2 Validation 3 Contacts 4 Confirm

Your CSR – or “Certificate Signing Request” – is base64 encoded data that contains a public key and information about the certificate applicant, such as organization, locality, state, country, and domain name for which the certificate should be issued. Usually, the CSR is generated server-side, along with the private key. Your CSR is required for activation of your SSL certificate. If you’re renewing an existing SSL certificate, you may use your previous CSR. However, that may create a security threat, so we recommend you get a new CSR every time. [Learn how to generate a CSR →](#)

Enter CSR

Primary Domain

Server Type

Hashing Algorithm

On vérifie les informations | **Next.**

Reissue PositiveSSL Certificate

1 CSR 2 Validation 3 Contacts 4 Confirm

Your CSR – or “Certificate Signing Request” – is base64 encoded data that contains a public key and information about the certificate applicant, such as organization, locality, state, country, and domain name for which the certificate should be issued. Usually, the CSR is generated server-side, along with the private key. Your CSR is required for activation of your SSL certificate. If you’re renewing an existing SSL certificate, you may use your previous CSR. However, that may create a security threat, so we recommend you get a new CSR every time. [Learn how to generate a CSR →](#)

Primary Domain

Server Type

Hashing Algorithm

Email

Company

Department

Location

Email | on choisit l'adresse courriel adéquate dans **Approver Email** | **Next.**

Product List → SSL Certificates → Activate

Activate PositiveSSL Certificate

1 CSR 2 Validation 3 Contacts 4 Confirm

A Domain Control Validation (DCV) method is necessary for security purposes. The Certificate Authority uses the DCV to verify that the person placing the request owns the domain and/or is authorized to use it.

DCV Method

Approver Email

The Certificate Authority will send a validation email (wherever applicable), and you'll need to click the included link to complete DCV.

Demander une certification à Namecheap

On vérifie | Next.

Reissue PositiveSSL Certificate

CSR Validation Contacts Confirm

Company Contacts USE ADDRESS BOOK CONTACT

You have the option to edit your Company Contacts at this time. If you previously entered information for an optional field, you'll need to fill in that field again for reissue. If you're applying as an individual, simply enter 'NA' in the Company Name field.

Company Name: NA
Department: NA
Company Number: NA
City of Incorporation: NA
State/Province of Incorporation: QC
Country of Incorporation: Canada
Address: [Redacted]
City: Montreal
State/Province: QC
ZIP/Postal Code: H3M 1L1
Country: Canada

Administrative Contacts

The Administrative Contact is the person who handles administrative duties, communicates with the Certificate Authority (CA), and receives the SSL certificate from the CA.

Email Address: [Redacted]
Certificate will be delivered to this address.

Next Cancel

On vérifie | Confirm.

Reissue PositiveSSL Certificate

CSR Validation Contacts Confirm

When you submit your info for this step, the activation process will begin and your SSL certificate will be available from your Domain List. To finalize the activation, you'll need to complete the Domain Control Validation process. Please follow the instructions below.

Email Validation Instructions

Shortly, an email will be sent to the specified address. Locate that email and click the link inside to finish the DCV process and activate your certificate.

Domain to Validate: www.micronator.org PRIMARY DOMAIN
via admin@micronator.org

Confirm Cancel

Need help? We're always here for you. [Chat with a Live Person](#)

Done.

Certificate Details: PositiveSSL ALERT
for www.micronator.org **COMODO** Creating Trust Online

Great! We initiated the activation of your certificate. To complete the process, you need to finalize the Domain Control Validation procedure. X

- If you're using email DCV method, follow instruction from the certificate authority in your inbox.
- If you're using HTTP-based DCV method, go to Certificate Details page to download the validation file.
- If you're using DNS-based DCV method, go to Certificate Details page to get the necessary host records.

[Read more in our knowledgebase](#)

Validity: Jan 23, 2016 - Jan 17, 2017
Validation Level: Domain Validation (DV)
Certificate Authority's ID: 20014385
Namecheap Order ID: [Redacted] [SEE ORDER](#)
Total Domains: 1 domain

Certificate Versions

Certificate ID	Status	Secured Domains
[Redacted]	IN PROGRESS	1 Domain SEE DETAILS

Done


Une nouvelle page s'affiche.

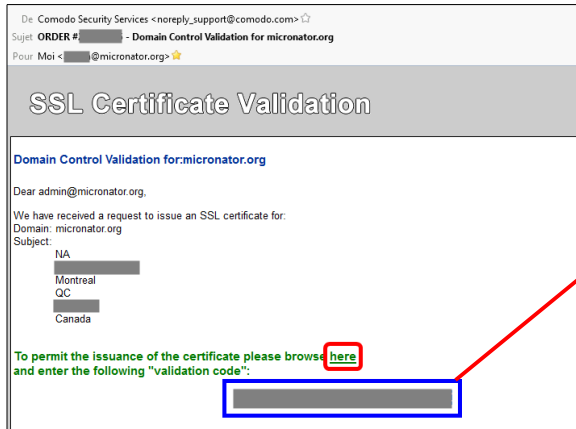
SSL Certificates

This page contains all your SSL certificates that require activation. To view your previously activated certificates, go to [Domain List](#)

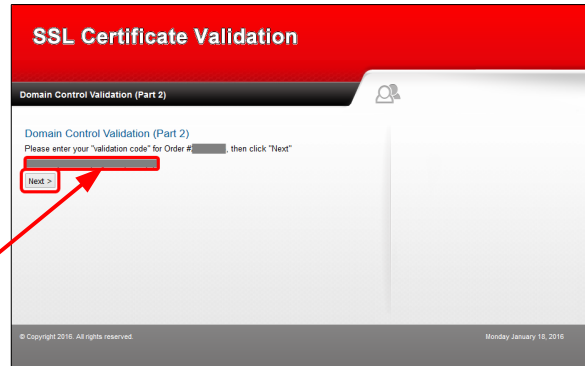
The list is empty.

6. Courriel et validation du certificat

 L'**usager admin du domaine** reçoit un courriel | on copie le "**validation code**" puis on clique [here](#).

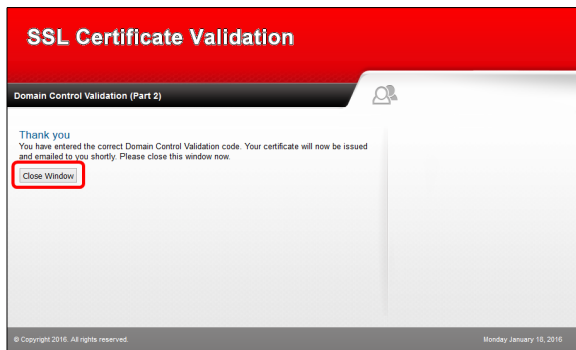


Chez namecheap.com, on colle le "**validation code**" | **Next**.

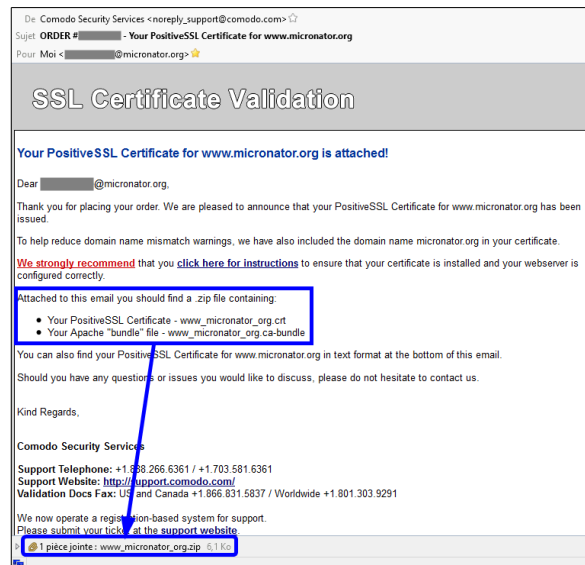


7. Réception du certificat

Close window.

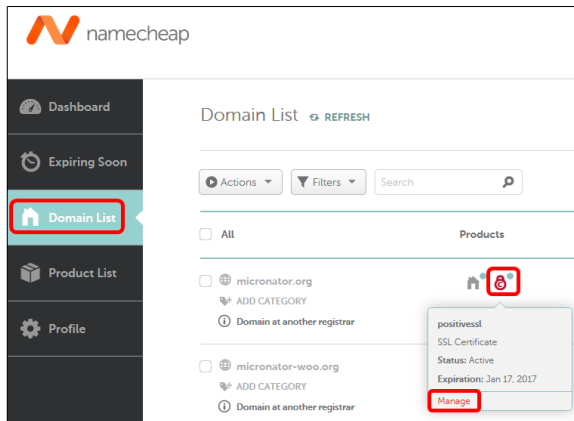


On reçoit un autre courriel avec un fichier zip contenant: notre certificat et un fichier "**bundle**" pour Apache. On sauvegarde le fichier ZIP.



8. Vérification du statut du certificat

Dashboard | **Domain List** | mettre la souris au-dessus du [petit cadenas](#) pour faire apparaître un menu | **Manage**.



Le statut de notre certificat chez **namecheap.com** a été changé pour **ISSUED**.

Certificate ID	Status	Secured Domains
[REDACTED]	ISSUED	1 Domain

Nous sommes prêts à installer notre nouveau certificat sur notre **Serveur SME**.

9. Installation du certificat



L'installation du certificat se fait de la même manière que celle de **GoDaddy**. Voir le chapitre [Installation](#) à la page [23](#).

IX- Réémission d'une certification Namecheap

1. Introduction

Il est parfois requis de réémettre le certificat pour une raison quelconque. Il n'en coûte rien pour réémettre un certificat. C'est presque exactement comme pour une première demande sauf pour le début des manipulations.

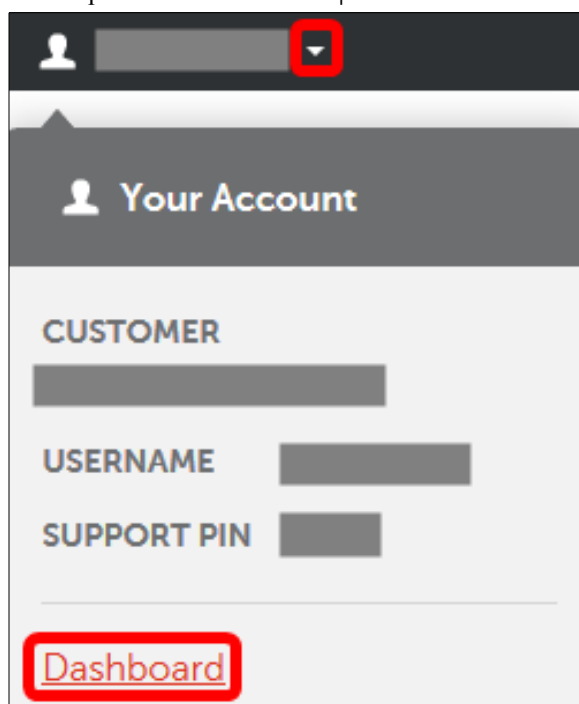
2. Création du fichier pour la requête CSR

💡 Pour **namecheap.com**, on utilise le répertoire de travail: **/root/CSR** pour créer la requête.

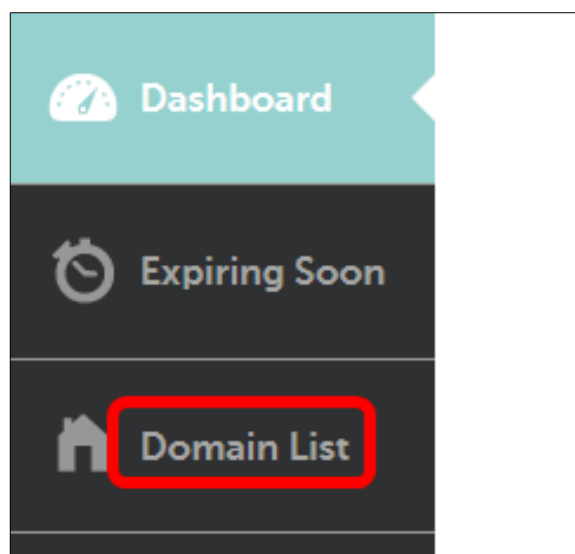
📄 La requête CSR pour **namecheap.com** est générée de la même manière que pour **GoDaddy**. Voir le chapitre [Création de la requête CSR](#) à la page 9. On peut aussi utiliser la même requête utilisée par **GoDaddy**.

3. Réémission

On se logue chez **namecheap.com** et en haut à gauche, sous notre identifiant, on clique la petite flèche pour dérouler le menu | **Dashboard**.



Domain List.



Réémission d'une certification Namecheap

On clique le cadenas pour faire dérouler le menu | **Manage**.

Domain List [REFRESH](#)

Actions ▾

All Products

micronator.org

ADD CATEGORY

Domain at another registrar

positivessl

SSL Certificate

Status: Active

Expiration: Jan 17, 2017

Manage

On clique **SEE DETAILS** pour faire dérouler le menu | **Reissue**.

Certificate Versions

Certificate ID	Status	Secured Domains	
	ISSUED	1 Domain	SEE DETAILS Reissue Download Certificate
	REPLACED	1 Domain	

Done

Yes.

Reissue PositiveSSL certificate

Please be aware: Once you begin the reissue process, you will no longer be able to download the old certificate. Do you wish to reissue?

Yes No

On colle notre fichier CSR | on choisit **Apache...** | **Submit**.

Reissue PositiveSSL Certificate

1 CSR 2 Validation 3 Contacts 4 Confirm

Your CSR – or “Certificate Signing Request” – is base64 encoded data that contains a public key and information about the certificate applicant, such as organization, locality, state, country, and domain name for which the certificate should be issued. Usually, the CSR is generated server-side, along with the private key. Your CSR is required for activation of your SSL certificate. If you’re renewing an existing SSL certificate, you may use your previous CSR. However, that may create a security threat, so we recommend you get a new CSR every time. [Learn how to generate a CSR →](#)

Enter CSR

```
iAgku2KtR2PA21b+BLDEa2if6OTObdqBvT0z5vsEUS8
P/TskmsfABnH77yFPh4
V2toqy+ED6zixW2X4yT9oipT4giP
/ujrhlTZOihD9o86c50EnlWm2G5bKUAFACT9j
6/CTXulZegWClSy9qOv56
/KueQf6Kli6EJ9YhqlqleDOFXSg7p82naxjvZ79PO
P409AyBsMMSdXT74MAx30sbrIP/+0kewyTK
```

CSR code content: Generate CSR Code here →

Primary Domain

Will be filled in automatically after CSR code has been inserted.

Server Type

Hashing Algorithm

Submit Cancel

On vérifie | Next.

Reissue PositiveSSL Certificate

1 2 3 4
CSR Validation Contacts Confirm

Your CSR – or ‘Certificate Signing Request’ – is base64 encoded data that contains a public key and information about the certificate applicant, such as organization, locality, state, country, and domain name for which the certificate should be issued. Usually, the CSR is generated server-side, along with the private key. Your CSR is required for activation of your SSL certificate. If you’re renewing an existing SSL certificate, you may use your previous CSR. However, that may create a security threat, so we recommend you get a new CSR every time. [Learn how to generate a CSR →](#)

Primary Domain

Server Type


Hashing Algorithm

Email

Company

Department

Location

 **Email** | on choisit le courriel dans *Approver Email* | Next.

Reissue PositiveSSL Certificate

1 2 3 4
CSR Validation Contacts Confirm

A Domain Control Validation (DCV) method is necessary for security purposes. The Certificate Authority uses the DCV to verify that the person placing the request owns the domain and/or is authorized to use it.

DCV Method

Approver Email

The Certificate Authority will send a validation email (wherever applicable), and you'll need to click the included link to complete DCV.

On vérifie | Next.

Reissue PositiveSSL Certificate

1 2 3 4
CSR Validation Contacts Confirm

Company Contacts USE ADDRESS BOOK CONTACT

You have the option to edit your Company Contacts at this time. If you previously entered information for an optional field, you'll need to fill in that field again for reissue. If you're applying as an individual, simply enter 'NA' in the Company Name field.

Company Name

Department

Company Number

City of Incorporation

State/Province of Incorporation

Country of Incorporation

Address

City

State/Province

ZIP/Postal Code

Country

Administrative Contacts

The Administrative Contact is the person who handles administrative duties, communicates with the Certificate Authority (CA), and receives the SSL certificate from the CA.

Email Address

Certificate will be delivered to this address.

On vérifie | Confirm.

Reissue PositiveSSL Certificate

1 2 3 4
CSR Validation Contacts Confirm

When you submit your info for this step, the activation process will begin and your SSL certificate will be available from your *Domain List*. To finalize the activation, you'll need to complete the Domain Control Validation process. Please follow the instructions below.

Email Validation Instructions

Shortly, an email will be sent to the specified address. Locate that email and click the link inside to finish the DCV process and activate your certificate.

Domain to Validate

Need help? We're always here for you.

Réémission d'une certification Namecheap

Done.

Certificate Details: PositiveSSL **ALERT** **COMODO**
Creating Trust Online
for **www.micronator.org**

Great! We initiated the activation of your certificate. To complete the process, you need to finalize the Domain Control Validation procedure. ✕

- If you're using email DCV method, follow instruction from the certificate authority in your inbox.
- If you're using HTTP-based DCV method, go to Certificate Details page to download the validation file.
- If you're using DNS-based DCV method, go to Certificate Details page to get the necessary host records.

[Read more in our knowledgebase](#) —

Validity: Jan 23, 2016 - Jan 17, 2017
Validation Level: Domain Validation (DV)
Certificate Authority's ID: 20014383
Namecheap Order ID: [REDACTED] [SEE ORDER](#)
Total Domains: 1 domain

Certificate Versions

Certificate ID	Status	Secured Domains	
[REDACTED]	IN PROGRESS	1 Domain	SEE DETAILS
[REDACTED]	USED	1 Domain	SEE DETAILS
[REDACTED]	REPLACED	1 Domain	SEE DETAILS
[REDACTED]	REPLACED	1 Domain	SEE DETAILS
[REDACTED]	REPLACED	1 Domain	SEE DETAILS

[Done](#)

Une nouvelle page s'affiche.

SSL Certificates

This page contains all your SSL certificates that require activation. To view your previously activated certificates, go to [Domain List](#) ->

The list is empty.

L'utilisateur admin reçoit un courriel | on copie le "validation code" puis on clique [here](#).

De: Comodo Security Services <noreply_support@comodo.com> ☆
Sujet: **ORDER # [REDACTED] - Domain Control Validation for www.micronator.org**
Pour: Moi <admin@micronator.org> ☆

SSL Certificate Validation

Domain Control Validation for: www.micronator.org

Dear admin@micronator.org,

We have received a request to issue an SSL certificate for:
Domain: www.micronator.org
Subject:
NA
[REDACTED]
Montreal
QC
[REDACTED]
Canada

To permit the issuance of the certificate please browse [here](#) and enter the following "validation code":

B2FG [REDACTED] Z8

On colle le "validation code" | Next.

SSL Certificate Validation

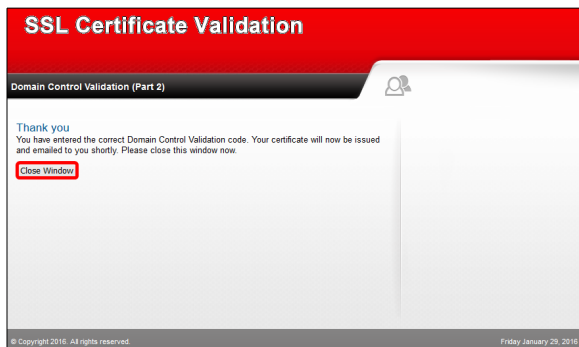
Domain Control Validation (Part 2)

Domain Control Validation (Part 2)
Please enter your "validation code" for Order # [REDACTED], then click "Next"

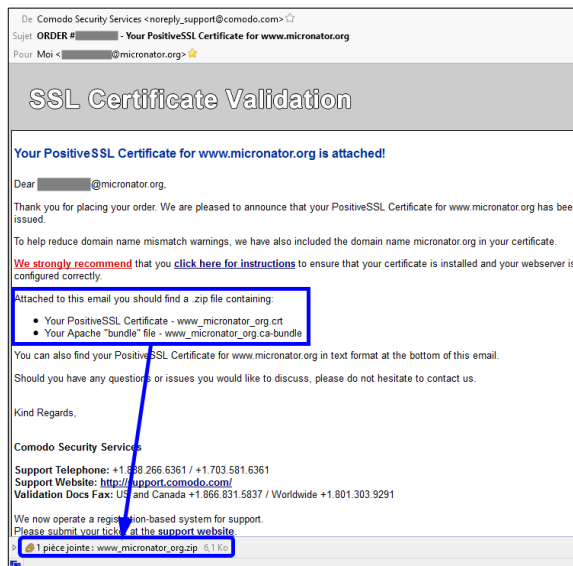
[Next >](#)

© Copyright 2016. All rights reserved. Friday, January 29, 2016

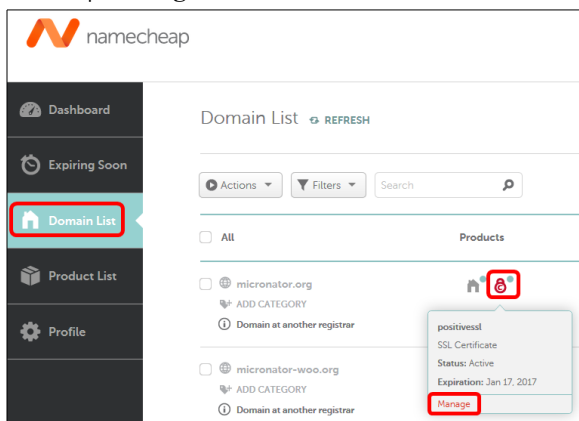
Close window.



- On reçoit un autre courriel avec un fichier **zip** contenant: notre certificat et un fichier "**bundle**" pour **Apache**.
- On sauvegarde le fichier ZIP, on le dézippe et on le transfert sur le serveur.



Dashboard | Domain List | passez la souris au-dessus du petit cadenas pour faire apparaître un menu | **Manage**.



- Le statut de notre certificat chez **namecheap.com** a changé pour devenir **ISSUED**.
- L'ancien certificat est devenu **REPLACED**.

Certificate ID	Status	Secured Domains
[redacted]	ISSUED	1 Domain
[redacted]	REPLACED	1 Domain
[redacted]	REPLACED	1 Domain



L'installation du certificat se fait de la même manière que celle de **GoDaddy**. Voir le chapitre [Installation](#) à la page [23](#).

4. Aide en ligne chez namecheap.com

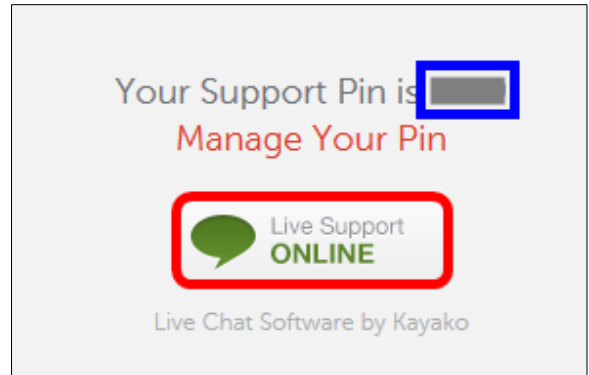
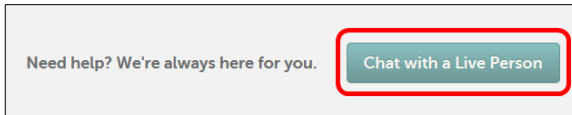
Si on rencontre un problème quelconque on peut toujours demande de l'aide en ligne. Les techniciens de **namecheap.com** sont toujours prêts à nous assister et ils répondent en quelques minutes seulement. Nous avons tenté l'expérience à plusieurs reprises et le service est impeccable.

On peut trouver l'icône de demande d'aide en ligne au bas de la plupart des pages du site.

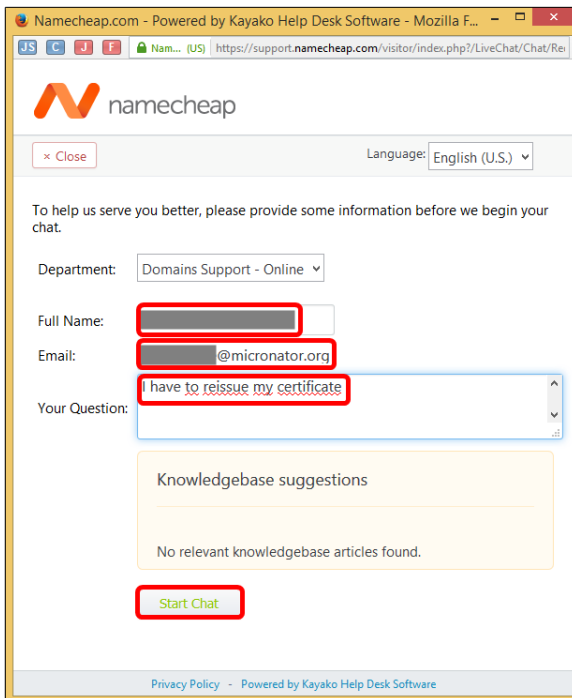
- Notre numéro de Pin apparaît à droite, on va vous le demander.

- On clique **Live Support ONLINE**.

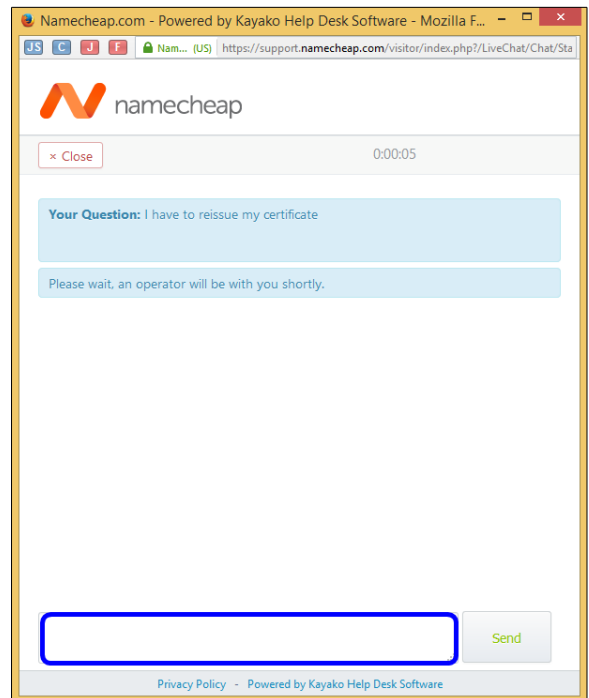
Chat with a Live Person.



On entre les informations demandées | **Start Chat.**



En quelques minutes, quelqu'un va nous répondre.



X- Création d'un certificat SME standard

1. Introduction

Si on veut recréer un certificat original émis et certifié par le **Serveur SME-9.1** lui-même, il suffit de suivre les instructions ci-dessous.

2. Création d'un répertoire de sauvegarde

Après s'être logué avec l'utilisateur **root**, on devrait être dans le répertoire personnel de ce dernier.

On vérifie.

```
[root@dorjee ~]# pwd
/root
[root@dorjee ~]#
```

On crée un répertoire de sauvegarde.

```
[root@dorjee ~]# mkdir Cert_org
[root@dorjee ~]#
```

On vérifie.

```
[root@dorjee ~]# ls -alsd Cert_org/
4 drwxr-xr-x 2 root root 4096 29 janv. 03:21 Cert_org/
[root@dorjee ~]#
```

On se rend dans le répertoire de sauvegarde.

```
[root@dorjee ~]# cd Cert_org/
[root@dorjee Cert_org]#
```

On vérifie.

```
[root@dorjee Cert_org]# pwd
/root/Cert_org
[root@dorjee Cert_org]#
```

3. Sauvegarde des fichiers du certificat actuel

Recherche des chemins des fichiers originaux du certificat.

```
[root@dorgee Cert_org]# cat /etc/httpd/conf/httpd.conf | grep SSLCertificate
SSLCertificateChainFile /home/e-smith/ssl.crt/gd_bundle-g2-g1.crt
SSLCertificateFile /home/e-smith/ssl.crt/dorgee.micronator.org.crt
SSLCertificateKeyFile /home/e-smith/ssl.key/dorgee.micronator.org.key
[root@dorgee Cert_org]#
```

3.1. On sauvegarde les fichiers originaux

```
[root@dorgee Cert_org]# cp /home/e-smith/ssl.crt/gd_bundle-g2-g1.crt .
[root@dorgee Cert_org]#
```

```
[root@dorgee Cert_org]# cp /home/e-smith/ssl.crt/dorgee.micronator.org.crt .
[root@dorgee Cert_org]#
```

```
[root@dorgee Cert_org]# cp /home/e-smith/ssl.key/dorgee.micronator.org.key .
[root@dorgee Cert_org]#
```

On affiche le fichier pem.

```
[root@dorgee Cert_org]# ls -als /home/e-smith/ssl.pem/
total 20
4 drwx----- 2 root root 4096 29 janv. 03:31 .
4 drwxr-xr-x 10 admin admin 4096 29 janv. 03:32 ..
12 -rw-r--r-- 1 root root 8738 27 janv. 10:31 dorgee.micronator.org.pem
[root@dorgee Cert_org]#
```

On sauvegarde le fichier pem.

```
[root@dorgee Cert_org]# cp /home/e-smith/ssl.pem/dorgee.micronator.org.pem .
[root@dorgee Cert_org]#
```

On vérifie les sauvegardes.

```
[root@dorgee Cert_org]# ls -als
total 36
4 drwxr-xr-x 2 root root 4096 29 janv. 03:40 .
4 drwxr-x--- 17 root root 4096 29 janv. 03:31 ..
4 -rw-r--r-- 1 root root 1858 29 janv. 03:25 dorgee.micronator.org.crt
4 -rw-r--r-- 1 root root 1704 29 janv. 03:26 dorgee.micronator.org.key
12 -rw-r--r-- 1 root root 8738 29 janv. 03:40 dorgee.micronator.org.pem
8 -rw-r--r-- 1 root root 4795 29 janv. 03:25 gd_bundle-g2-g1.crt
[root@dorgee Cert_org]#
```

4. Effaçage des fichiers du certificat

Référence:

http://wiki.contribs.org/Useful_Commands#How_to_simply_recreate_the_certificate_for_SME_Server.

On efface tous les certificats.

```
[root@dorgee ~]# rm /home/e-smith/ssl.crt/*

rm : supprimer fichier « /home/e-smith/ssl.crt/dorgee.micronator.org.crt » ? y
rm : supprimer fichier « /home/e-smith/ssl.crt/gd_bundle-g2-g1.crt » ? y
[root@dorgee ~]#
```

On efface toutes les clés.

```
[root@dorgee ~]# rm /home/e-smith/ssl.key/*

rm : supprimer fichier « /home/e-smith/ssl.key/dorgee.micronator.org.key » ? y
[root@dorgee ~]#
```

On efface tous les fichiers pem.

```
[root@dorgee ~]# rm /home/e-smith/ssl.pem/*

rm : supprimer fichier « /home/e-smith/ssl.pem/dorgee.micronator.org.pem » ? y
[root@dorgee ~]#
```

On efface le lien du fichier de la chaîne de certificats.

```
[root@dorgee ~]# config delprop modSSL CertificateChainFile
[root@dorgee ~]#
```

On efface le Nom Commun.

```
[root@dorgee ~]# config delprop modSSL CommonName
[root@dorgee ~]#
```

On efface le lien des fichiers des certificats.

```
[root@dorgee ~]# config delprop modSSL crt
[root@dorgee ~]#
```

On efface le lien des fichiers des clés.

```
[root@dorgee ~]# config delprop modSSL key
[root@dorgee ~]#
```

On vérifie avec modSSL.

```
[root@dorgee ~]# modSSL=service
```

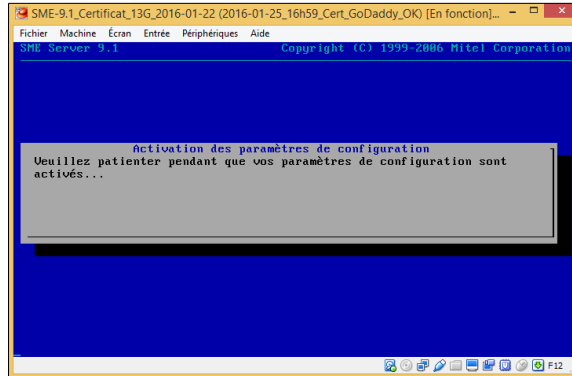
5. Signalement des modifications et réamorçage

```
[root@dorgee ~]# signal-event post-upgrade ; signal-event reboot

Broadcast message from root@dorgee
(/dev/pts/0) at 4:56 ...

The system is going down for reboot NOW!
[root@dorgee ~]#
```

Avec le réamorçage, le serveur active les nouveaux paramètres de configuration du certificat.



6. Vérification

On se relogue et on vérifie le fichier du certificat.

```
[root@dorgee ~]# ls -als /home/e-smith/ssl.crt/

total 12
4 drwx----- 2 root root 4096 29 janv. 05:18 .
4 drwxr-xr-x 10 admin admin 4096 29 janv. 05:19 ..
4 -rw-r--r-- 1 root root 1510 29 janv. 05:18 dorgee.micronator.org.crt
[root@dorgee ~]#
```

On vérifie la clé du serveur.

```
[root@dorgee ~]# ls -als /home/e-smith/ssl.key/

total 12
4 drwx----- 2 root root 4096 29 janv. 05:18 .
4 drwxr-xr-x 10 admin admin 4096 29 janv. 05:19 ..
4 -rw-r--r-- 1 root root 1676 29 janv. 05:18 dorgee.micronator.org.key
[root@dorgee ~]#
```

On vérifie le fichier pem.

```
[root@dorgee ~]# ls -als /home/e-smith/ssl.pem/

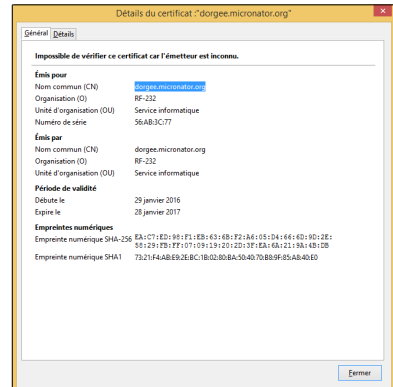
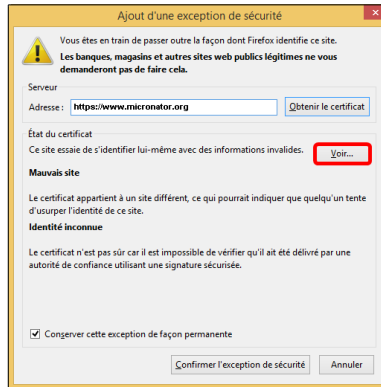
total 12
4 drwx----- 2 root root 4096 29 janv. 05:18 .
4 drwxr-xr-x 10 admin admin 4096 29 janv. 05:19 ..
4 -rw-r--r-- 1 root root 3568 29 janv. 05:18 dorgee.micronator.org.pem
[root@dorgee ~]#
```

On vérifie avec modSSL.

```
[root@dorgée ~]# modSSL=service
[root@dorgée ~]#
```

Avec un fureteur, on va à <http://www.micronator.org>.

Je comprends les risques | Ajouter une exception... | Voir... Le certificat avec les paramètres originaux a été recréé.



On ferme tout.

Le nouveau certificat émis et certifié par le **Serveur SME-9.1** lui-même est fonctionnel.



Victoire totale, hissons la bannière de la victoire.

Crédits

© 2016 RF-232

Auteur: **Michel-André Robillard CLP**

Remerciement: **Tous les contributeurs GNU/GPL.**

Intégré par: **Michel-André Robillard CLP**

Contact: **michelandre at micronator.org**

Répertoire de ce document: E:\000_DocPourRF232_general\RF-232_SME-9.1_Certificat-SSL\RF-232_SME-9.1_Certificat-SSL_2016-01-31_10h31.odt

Historique des modifications:

<i>Version</i>	<i>Date</i>	<i>Commentaire</i>	<i>Auteur</i>
0.0.1	2016-01-17	Début.	M.-A. Robillard
0.0.2	2016-01-31	Correction pour le choix du fichier CSR lors d'une réémission. Ajout d'une note et d'un lien vers le serveur virtuel de test.	M.-A. Robillard

Index

2		
2048 bits.....	12	
A		
À savoir.....	7	
accents.....	11, 12	
Achat du certificat.....	14	
ACTIVATE.....	47	
Activation du certificat.....	46	
Add to Cart.....	14, 44	
admin@nom-du-domaine.....	8	
Afficher le certificat.....	35	
Afficher le statut.....	21	
Aide en ligne.....	57	
Ajouter une exception.....	33	
Allow in the future.....	38	
American Express.....	6	
Apache.....	10, 17, 48	
Apache version < 2.4.8.....	23	
Apache version 2.4.8+.....	23	
apache-2.4.0.....	23	
Apparence.....	40	
Approver Email.....	48, 54	
ASCII.....	5	
astérisque (*).....	12	
astuce.....	5	
Avast pour EI.....	37	
Avertissement.....	2	
B		
BD de SME.....	31	
BEGIN et END.....	15	
bleu.....	5	
Bloc-notes.....	40	
Boutique de Micronator.....	6	
Brancher les aînés.....	6	
bundle.....	28	
Bundle.....	25	
C		
C=.....	9	
CA.....	11	
cadenas.....	34	
caractère spécial.....	11	
cat.....	15	
Certificat GoDaddy.....	29	
Certificat GoDaddy.com.....	7	
Certificat namecheap.com.....	8	
certificat SSL.....	12	
CERTIFICAT SSL.....	17	
certificat SSL de GoDaddy.....	14	
certificat X.509.....	9	
Certificate Signing Request.....	9	
CertificateChainFile.....	31	
chaîne de certification.....	28	
Chaîne de certification.....	30	
Challenge password.....	11	
Changer le site.....	20	
Chat with a Live Person.....	57	
chmod ug+w.....	41	
Choix du certificat.....	44	
Clé privée.....	30	
clé privée du Serveur SME.....	13	
CN=.....	9	
code à deux lettres ISO.....	9	
Code de validation.....	7, 8	
code pour le sceau.....	40	
Commentaire.....	63	
Commentaires et suggestions.....	6	
Common Name.....	11	
CommonName.....	31	
config delprop.....	60	
config show modSSL.....	31	
Configuration du certificat.....	15	
Confirm Order.....	44	
Contact.....	16	
Conventions.....	5	
Country Name.....	11	
Courriel du certificat.....	16	
courriels du certificat.....	7	
Cpanel.....	48	
CR.....	5	
Create account.....	44	
Création d'un certificat.....	58	
Création d'un certificat SME standard.....	8	
création d'un compte.....	44	
Création de la requête.....	12	
Création de la requête CSR.....	19	
création du fichier pem.....	32	
Crédits.....	63	
crt.....	31	
D		
Dashboard.....	46	
delprop.....	60	
DÉSACTIVER.....	18	
Description générale.....	5	
Détails.....	36	
directive SSLCertificateChainFile.....	24	
Directive SSLCertificateChainFile	25	
Directive SSLCertificateFile.....	24	
Directive SSLCertificateKeyFile.....	24	
Discover.....	6	
DNS.....	11	
Domain List.....	51	
droit d'écriture.....	41	
E		
Effaçage des fichiers.....	60	
Email.....	48	
Émetteur.....	37	
Emplacement des fichiers.....	26	
Enable protection.....	38	
Enregistrer le fichier.....	22	
étape.....	5	
exception de sécurité.....	34	
Explorateur Internet.....	37	
F		
fichier "bundle" pour Apache.....	50	
fichier pem.....	30, 59	
Fichier ZIP du certificat.....	7, 8	
fichiers du certificat actuel.....	59	
fichiers originaux.....	59	
FileZilla.....	29	
footer.php.....	41	
FQDN.....	9	
G		
Gérer.....	19	
gestion du certificat.....	19	
Get Started.....	7, 15	
GoDaddy SHA-2.....	16	
GoDaddy.com.....	7	
Google Chrome.....	36	
Google: godaddy ssl certificate.....	14	
H		

Index

here.....	50	nom réel de votre domaine.....	11	rpm -qa grep apache.....	23	
homme-entre-les-deux.....	37	non vérifié.....	5	RSA de 2048 bits.....	12	
Hosting Agreement.....	14	NON-RESPONSABILITÉ.....	2	rsa:2048.....	12	
I						
icône >.....	34	note.....	5	S		
infrastructure à clés publiques.....	9	NotePad++.....	40	S=.....	9	
Installation.....	23	Notes au lecteur.....	5	Sceau de sécurité.....	7, 40	
Introduction théorique.....	23	O				
ISO.....	9	O=.....	9	Se connecter.....	15	
ISSUED.....	51	openssl.....	12	sealID.....	41	
J						
Je comprends les risques.....	33	openssl list-public-key-algorithms.....	24	Secure Certificate Authority.....	35	
K						
key.....	31	optional company name.....	11	Secure Sockets Layer.....	23	
L						
L=.....	9	Options.....	17	Security.....	39	
La clé originale.....	27	orange.....	5	SEE DETAILS.....	53	
Le certificat original.....	28	Organization Name.....	11	Sélectionnez la longueur.....	18	
Le fichier pem original.....	28	Originaux.....	27	signal-event domain-modify.....	31	
LF.....	5	P				
lien here.....	8	Paiement.....	45	signal-event email-update.....	31	
Live Support ONLINE.....	57	paire de clés.....	9	signal-event post-upgrade.....	31, 61	
Login chez GoDaddy.....	19	paramètres DH.....	24	signal-event reboot.....	31, 61	
M						
magenta.....	5	Particularités de ce document.....	5	Signalement.....	61	
man in the middle.....	37	PayPal.....	6, 45	Signature de certificat.....	20	
Manage.....	51	PDF.....	5	Soumettre toutes les modifications.....	20	
Manipulation.....	5	Personnaliser.....	18	SSL Certificates.....	46	
MasterCard.....	6	Pied de page du thème.....	40	SSL v3.....	23	
Mes produits.....	17	PKCS#10.....	9	ssl_module.....	23	
Mettre à jour le fichier.....	41	PKI.....	9	ssl.crt.....	60	
micronator.org.....	6	Plus d'informations.....	35	ssl.key.....	60	
mkdir CSR.....	10	Private Policy.....	14	ssl.pem.....	59	
mod_ssl.c.....	23	procédure.....	5	SSLCACertificatePath.....	23	
modSSL.....	60	Proceed to Checkout.....	14	SSLCertificateChainFile.....	23, 25	
modSSL=service.....	60	Product List.....	46	SSLCertificateFile.....	23	
Module Apache mod_ssl.....	23	Public Key Infrastructure.....	9	SSLCertificateKeyFile.....	23	
mot de passe.....	10, 12	PuTTY.....	15, 26, 47	Start Chat.....	57	
N						
Namecheap.....	43	R				
Nginx.....	48	réamorçage.....	61	store-wp-enfant.....	41	
Nom Commun.....	11, 31	recommandation.....	5	Submit.....	45	
Nom du domaine.....	11	Réémission.....	52	T		
Tableau de bord.....						40
Téléchargement du certificat.....						17
Télécharger.....						21
Terms of Services.....						44
Thème enfant.....						40
TOR.....						38
tout-en-un.....						25
Transport Layer Security.....						23
trouble majeur avec un certificat... ..						8
Type de serveur.....						17
U						
Universal Terms of Service Agreement.....						14

Index

usager admin.....	8	WinSCP.....	29	[
usager root.....	10	WordPress HTTPS.....	34	[CTL] + [c].....	15, 40, 47
usager titulaire du compte.....	7	wwwmicronator.org.csr.....	15	@	
V		X		@, #, &, !.....	11
validation code.....	8, 50, 55	X.509.....	9, 24	/	
Vérification.....	33	-		/etc/hosts.....	11
Vérification avec Firefox.....	33	-keyout.....	12	/root/CSR.....	47
Version du serveur web.....	23	-newkey.....	12	/root/GoDaddy.....	29
Victoire.....	62	-nodes.....	12	©	
View certificate.....	36	-out.....	12	© RF-232.....	2
Visa.....	6				
Voir.....	33				
W		(
WebMail.....	16	(w).....	41		