http://WWW.CABARE.NET ©

Certificat SSL Wistee - Gandi – Cours & TP -

Tutoriel site Web (Gandi Simple Hosting) – RDS (Windows Server 2016 - 2012)

Michel Cabaré – Ver 1.0 – Juillet 2017-

Certificats SSL Wistee - Gandi
Tutoriel Site Web (Gandi Simple Hosting) – RDS (Windows Server 2016 - 2012)

Michel Cabaré – Ver 1.0 – Juillet 2017

www.cabare.net ©

TABLE DES MATIÈRES

SSL ET SITE WEB

Pourquoi du SSL sur un site WEB:

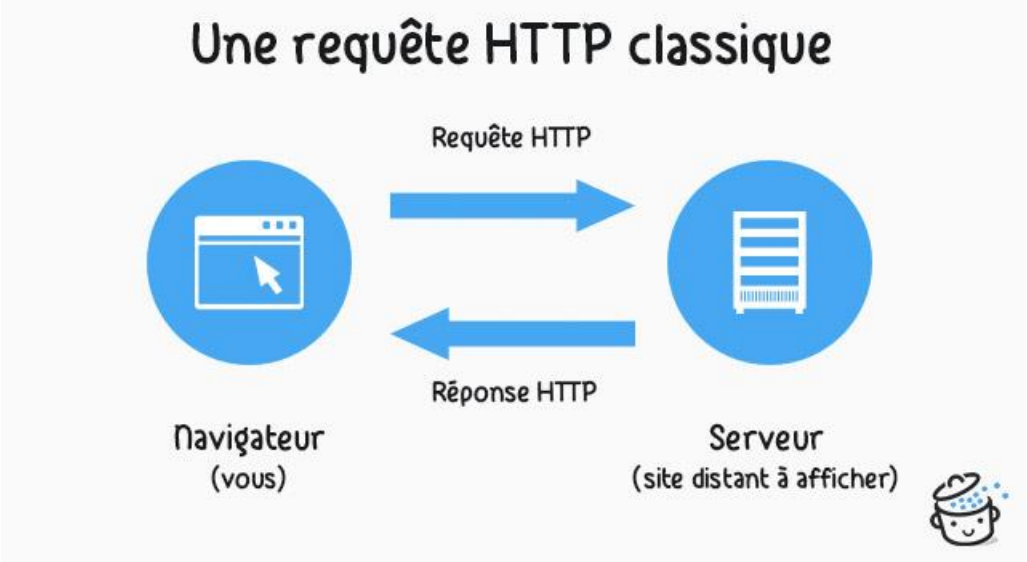
Depuis août 2014, Google communique sur l'importance des sites en **HTTPS** (c'est-à-dire avec la présence d'un **certificat SSL**). Avoir un site en **HTTPS** est devenu un critère de pertinence dans l'algorithme de Google : les sites sécurisés ont pu constater un meilleur positionnement dans les résultats de recherche du moteur.

Jusqu'à maintenant, l'impact était minime, n'affectant que 1% des requêtes mais il semblerait que les choses s'accélèrent

- Google vient d'annoncer un changement majeur dans sa politique d'indexation des pages web : désormais, si une page existe en HTTP et en HTTPS, c'est cette dernière qui sera indexée. Une manière de sécuriser le web avec un protocole plus sûr que le http

Fonctionnement en http sur un site WEB:

Dès que vous entrez une adresse dans votre navigateur, il envoie une requête HTTP pour demander la page. Le serveur la renvoie et le navigateur l'affiche



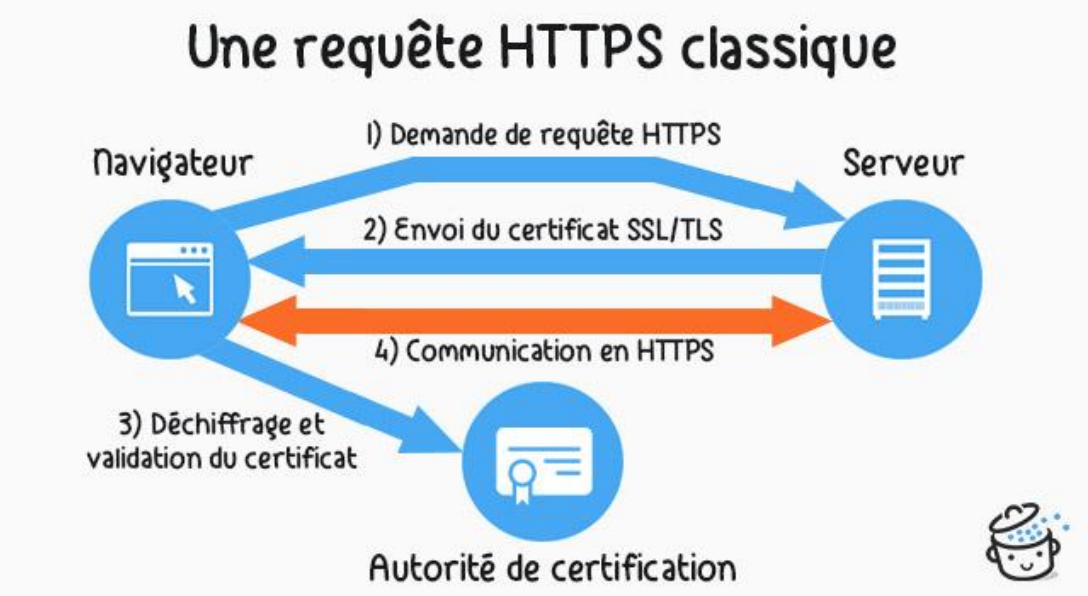
Fonctionnement en https – SSL sur un site WEB:

On retrouve souvent l'appellation **SSL** sur le web mais c'est un abus de langage. En fait, **SSL (Secure Socket Layer)** est la première version de ce protocole de sécurisation. **TLS (Transport Layer Security)** ayant pris le relais maintenant pour plus de sécurité.

Pour le **HTTPS**, d'autres acteurs entrent en scène mais nous allons retenir le principal : **l'autorité de certification**.

Ce genre d'organisme, également appelé également tiers de confiance, délivre un certificat SSL/TLS pour que les créateurs de sites puissent mettre en

place le HTTPS. Il en existe des dizaines d'autorités de certification mais les plus connues sont **Comodo**, **Thawte** , **GlobalSign**…



Certificats SSL – DV – OV- EV:

- **Les certificats à validation de domaine (DV)** : Dans ce cas, l'autorité de certification vérifiera jusque que vous êtes bien propriétaire du nom de domaine pour vous accorder le petit cadenas vert (la vérification se passe automatiquement en ligne) ;
- **Les certificats à validation de l'organisation (OV)** : Pour obtenir ce type de certificat, vous devez prouver que vous êtes la personne morale détentrice du domaine à sécuriser et fournir des documents papier comme un extrait KBIS ou une attestation de domiciliation (cela prendra donc un peu plus de temps) ;
- **Les certificats à validation étendue (EV)** : Ici, c'est plus sérieux. Pour obtenir ce genre de certificat, il faudra montrer patte blanche. Les informations que vous transmettrez sur votre organisation seront vérifiées (existence légale, physique, numéro de téléphone, adresse, activité, etc) et auditées chaque année.

  Ces derniers permettent de renforcer la confiance des visiteurs

Redirection 301 – permanente – (http sur https):

Une redirection 301 est une substitution permanente de l'adresse initialement demandée par l'adresse obtenue.

Une **redirection 301** est également appelée **redirection web** ou **redirection permanente** (*moved permanently),* une redirection permanente force votre navigateur web en charge de consulter un contenu à une adresse donnée sur internet à vous présenter un contenu provenant d'une autre adresse web. Ce qui nous intéressera cela sera de faire une redirection des adresses en **http** vers leur équivalente mais en **https** !

Eviter les redirections Javascript *(peuvent être assimilées à du spam)* et la balise méta « refresh ». Pour rediriger l'ensemble des pages de votre site de l'http vers l'https (SSL) :

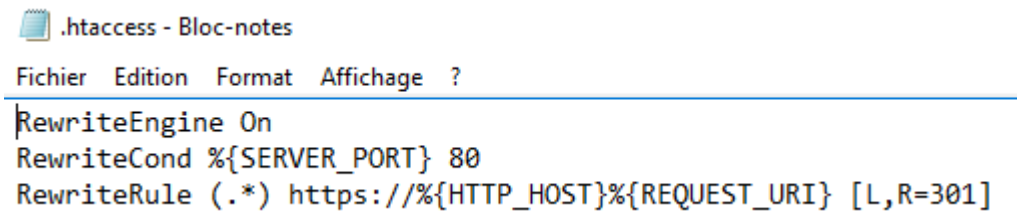
Si le port utilisé est le 80 (http), nous redirigeons le visiteur vers la version sécurisée 443 (https://) en conservant l'adresse de la page.

RewriteEngine On

RewriteCond %{SERVER_PORT} 80

RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]

Comme dans



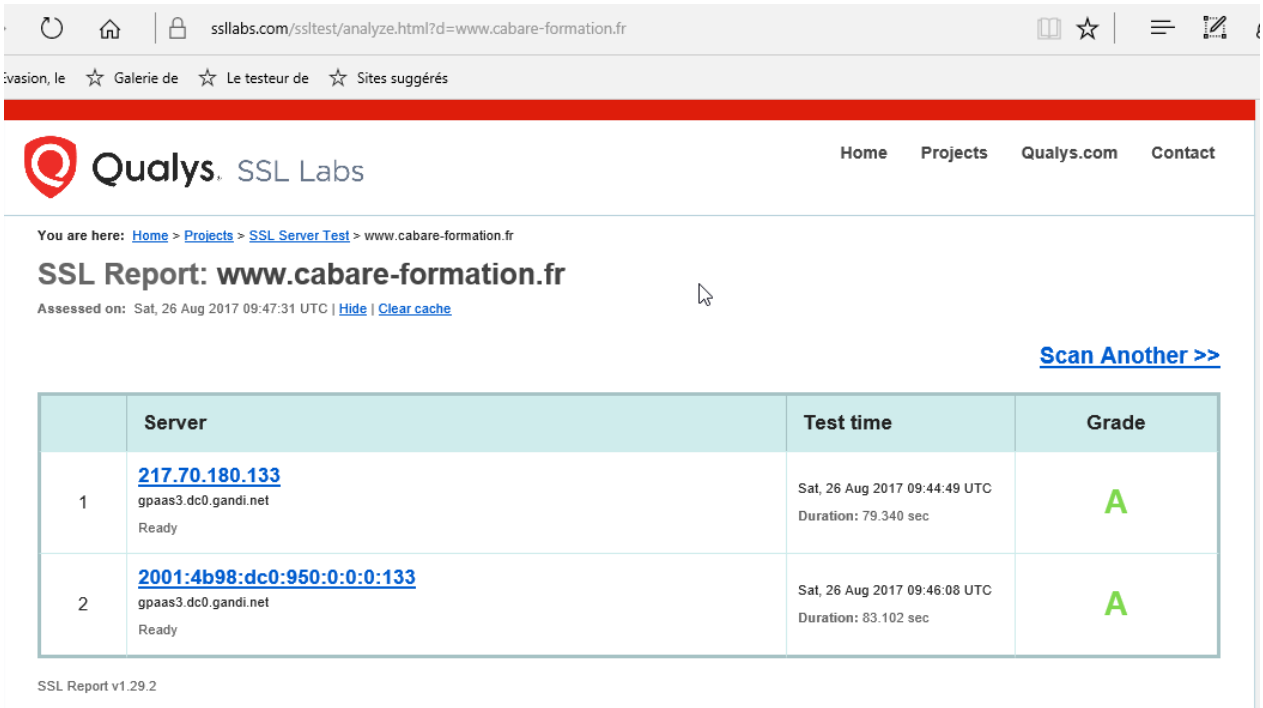
N.B: Si le port utilisé n'est pas le port 80 (?) alors on peut écrire la condition suivante

RewriteCond %{HTTPS} !=on

La condition %{HTTPS} !=on signifie « l'URL est demandée sans le protocole HTTPS ». On peut aussi tester **RewriteCond %{HTTPS} off**

N.B: penser également dans le cas d'une migration complète de site web à

- Changer les liens internes éventuels en dur
- Changer les liens aux CSS et bibliothèques
- Refaire et publier un Sitemap
- Reconstruire un Site dans les outils de supervision Google



CERTIFICATS WISTEE

Offre possible:

Bien de choses interviennent, notamment multi domaine, muli-sous domaine, compatibilité outils Mobiles, Barre de confiance, 2 sont intéressants

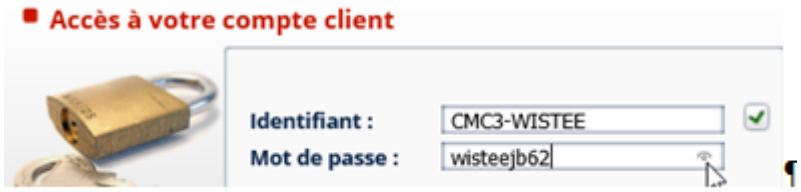
- Pour les solutions RDS, on n'a pas besoin de compatibilité outils portables, l'offre **WISTEE SSL DV** est correcte (25 euro…)
- Pour un site Web, on a besoin de compatibilité outils portables, et un affichage de logo Sceau de sécurité est rassurante, l'offre **Thawte SSL 123** est correcte (65 euro…)

N.B: la barre verte niveau sécurity **EV Extended Validation** est à 200 Euro…

CARACTÉRISTIQUES DU CERTIFICAT SSL	wistee SSL DV	thawte SSL 123
Chiffrement SSL	jusqu'à 256 Bits Clé RSA 2048 Bits ou supérieur	jusqu'à 256 Bits Clé RSA 2048 Bits ou supérieur
https:// + Cadenas de sécurité	✔	✔
Emis au nom du propriétaire (OV / EV)	✘	✘
Exemple de barre d'adresse URL Suppression du "Non Sécurisé" de Google Chrome	Sécurisé https://c	Sécurisé https://c
Nombre d'adresses sécurisables	1	1
Protocoles	SSL / TLS	SSL / TLS
Cryptographie	RSA / DSA	RSA / DSA
Compatibilité Navigateurs	+ 99%	+ 99%
Compatibilité Outils Mobiles	✘	✔
Garantie financière	$10.000 USD	$500.000 USD
INCLUS AVEC LE CERTIFICAT SSL		
Réémission gratuite	✘	✔
Satisfait ou Remboursé 30 Jours	✔	✔
Installation du certificat SSL par Wistee ®	Offert !	Offert !
Aide à l'installation, support et suivi personnalisé	✔	✔
Améliore le référencement SEO Google	✔	✔
Sceau de sécurité	✘	Secured by thawte 2005-00-00

Login Wistee:

Login **CMC3-WISTEE** Mdp **wisteeJb62**



LOGIQUE PROCEDURE CERTIFICATS

Procédure pour certificat SSL

2 temps sont nécessaires, demande de création du certificat, puis installation / activation

- D'abords il faut demander un certificat auprès d'une **CA Autorité de Certification**, via une requête **CSR** (**Certificate Signing Request**)
- Puis une fois le **certificat SSL** émis par le **CA** il faut le récupérer
- Une fois récupéré le **certificat SSL** il faut
  - l'installer sur le serveur voulu
  - l'activer pour l'application SSL

Demande CSR de certificat

La demande de certificat auprès d'une **CA Autorité de Certification**, via une requête **CSR** (**Certificate Signing Request**) varie selon si elle est effectuée depuis une machine Windows, ou linux

Depuis une machine Windows – (CSRW)

On travaille depuis **l'interface IIS**

On peut faire la demande **CSR** depuis le serveur IIS sur lequel on souhaite installer le certificat (même si on pourrait effectuer aussi la commande en invite de commande Open SSL)

La **clé privée** est gardée "dans le serveur" (et non pas stockée dans un fichier a part) on obtient un fichier "public" **.cer** ou **.txt** qui contient notre identification et notre demande de certificat, qu'il faudra envoyer à l'autorité de Certification.

Depuis une machine Linux – (CSRL)

On travaille en invite de commande avec la **commande OPENSSL**

On peut faire la demande **CSR** depuis le serveur **Gandi Simple Hosting** sur lequel on souhaite installer le certificat à travers une **console SSH** (permettant ensuite de passer la commande OpenSSL, mais aussi toutes les commandes souhaitées d'ailleurs)

On obtient la **clé Privée** au format **.key** (associée à un mot de passe) et un fichier "public" **.cer** qui contient notre identification et notre demande de certificat, qu'il faudra envoyer à l'autorité de Certification.

Récupération du Certificat SSL émis par le CA

On peut recevoir de la part de l' **Autorité de Certification** le certificat sous différents formats. Plus exactement, on est jamais en lien direct avec l'Authorité de certification, mais plutôt simplement par le fournisseur du certificat. Evidemment les procedures et les formats peuvent différer un peu selon le prestataire :

Via Wistee

Reception par mail

Via Gandi

Reception via l'interface du site gandi

Installation du Certificat SSL reçu (et activation application SSL)

On a recu de la part de l' **Autorité de Certification** le certificat sous différents formats :

Sur une machine Windows

Si on a généré la requête CSR sur IIS la clé privée est déjà présente sur le serveur windows,

Il ne reste plus qu'à importer alors le certificat "concaténé"

- cela peut se faire depuis IIS avec un certificat au format PKCS#7.
- Cela peut se faire sur RDS avec un certificat au format pfx (x509)

Et ensuite activer ce certificat pour le port 443 SSl du site Web par défaut

Sur une machine Gandi instance Simple Hosting - Linux

On dispose dans 2 fichier la clé privée et le certificat obtenu

Il faudra copier le contenu de ces fichier dans l'interface d'activation via le Site Web de Gandi

CERTIFICAT WISTEE SUR SERVEUR WINDOWS

Demande de certificat CSR – via Windows CSRW

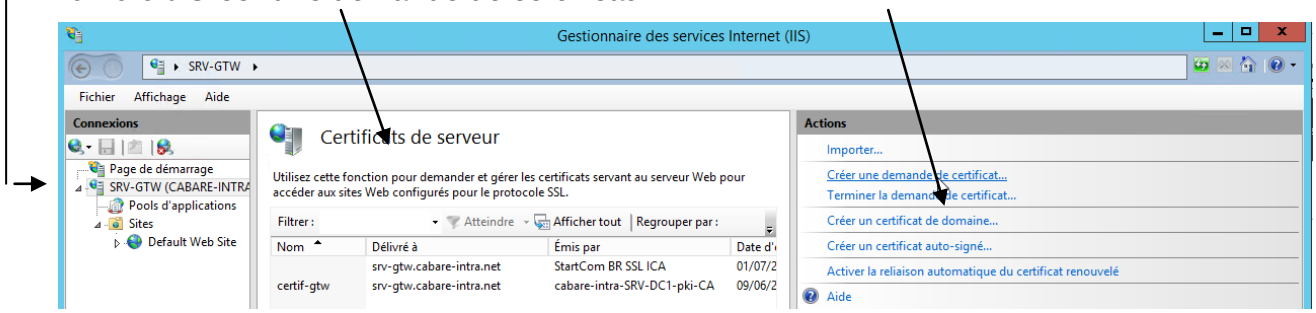
On peut faire la demande CSR depuis le serveur IIS sur lequel on souhaite installer le certificat

Dans ce cas la clé privée est gardée "dans" le serveur IIS et n'est pas obtenue dans un fichier à part.

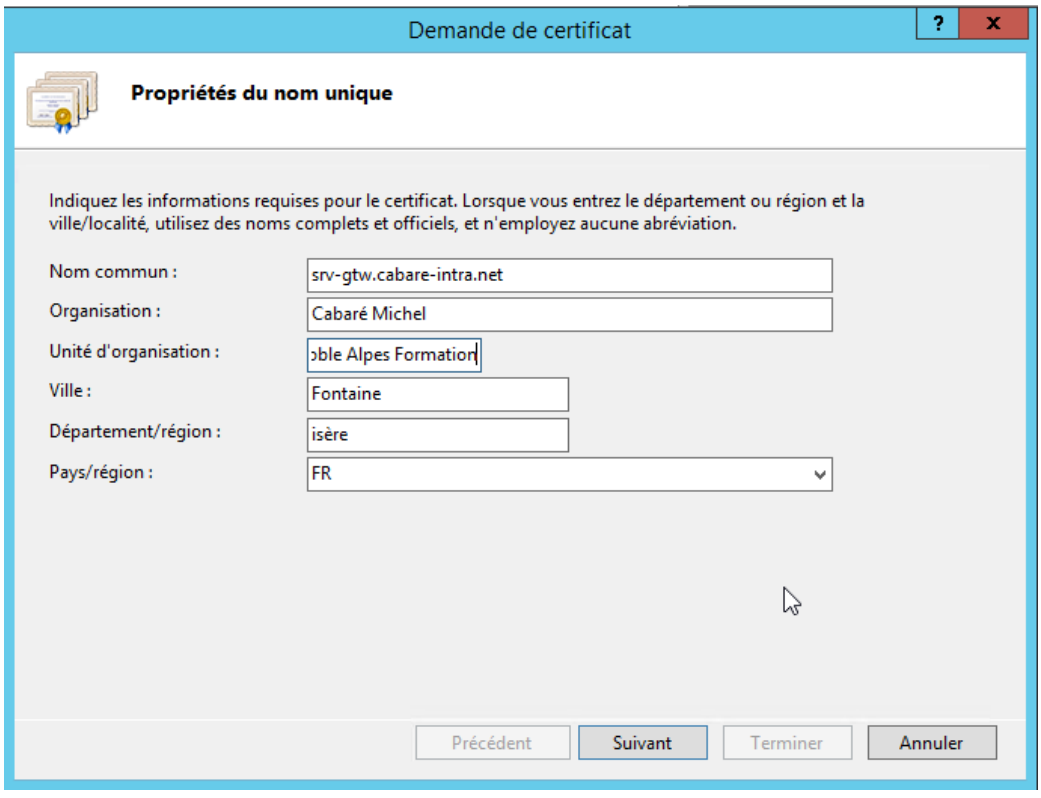
On a uniquement dans les "mains un fichier clé publique **.cer** contenant nos demandes d'identification et notre demande de certificat

demande depuis **Windows Internet Server**

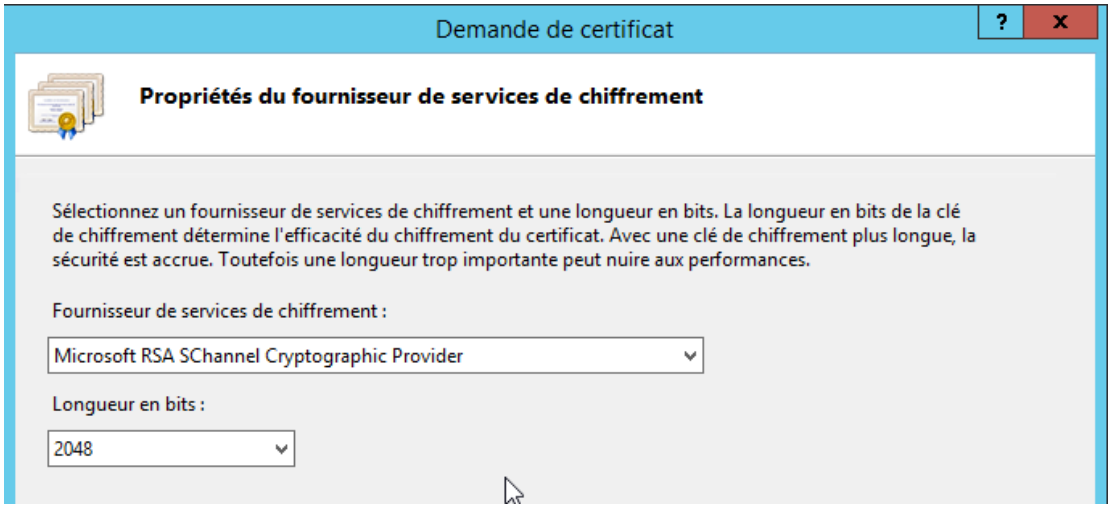
Sur **IIS**, on se place sur le serveur, on demande **Certificats de serveur**, puis on fait alors **Créer une demande de certificat**



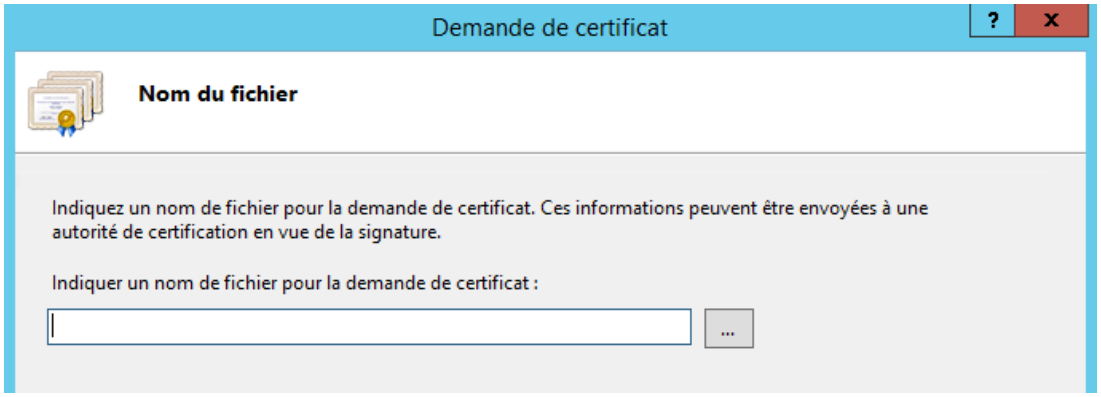
Un boite de dialogue s'ouvre alors, dans laquelle il faut faire très attention au nom commun,



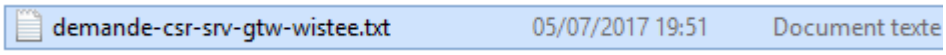
Il faut ensuite choisir **RSA** et **2048** comme longueur de clé de cryptage



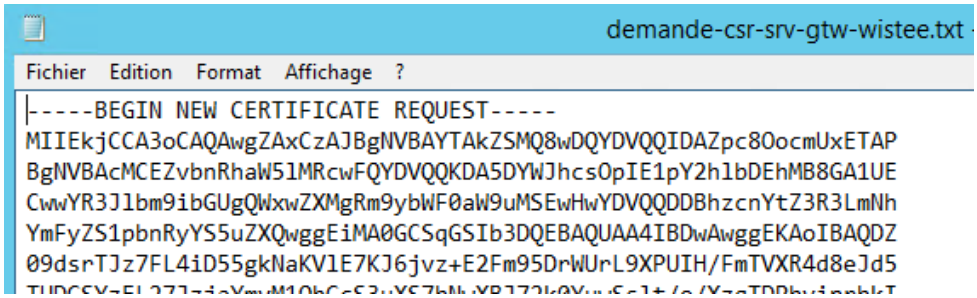
Et ensuite on pose le CSR où l'on veut



Pour obtenir la clé publique **.cer**



Ce fichier contient la demande de certificat, clé publique codée



Envois Demande de certificat CSR par mail a WISTEE

Il faut envoyer la **demande de certificat CSR** par mail à WISTEE pour que la demande soit traitée…

De : Christophe KASSE - Wistee.fr [mailto:c.kasse@wistee.fr]
Envoyé : mercredi 5 juillet 2017 19:40
À : michel@cabare.net
Objet : [WISTEE] Commande du certificat SSL "Certificat SSL : 30 Jours d'essai"

Bonjour,

Je fais suite à votre commande n°BC20170[illegible]950030, concernant l'émission d'un certificat SSL « Certificat SSL : 30 Jours d'essai »

Afin de pouvoir traiter votre demande, nous vous remercions de bien vouloir générer une Requête de Signature de Certificat (CSR) et de nous la faire parvenir en réponse à cet e-mail.

Traitement de la Demande de certificat par WISTEE

Wistee va instancier la demande de certificat, et on doit valider l'appartenance/propriété du domaine via un mail de confirmation (exemple)

De : sslorders@geotrust.com
À : webmaster@cabare-intra.net
Cc :
Objet : [14993288381] Approbation pour srv-gtw.cabare-intra.net

Cher,

vous avez reçu cet e-mail parce que vous êtes listé en tant que propriétaire du domaine srv-gtw.cabare-intra.net.

https://srv-gtw.cabare-intra.net

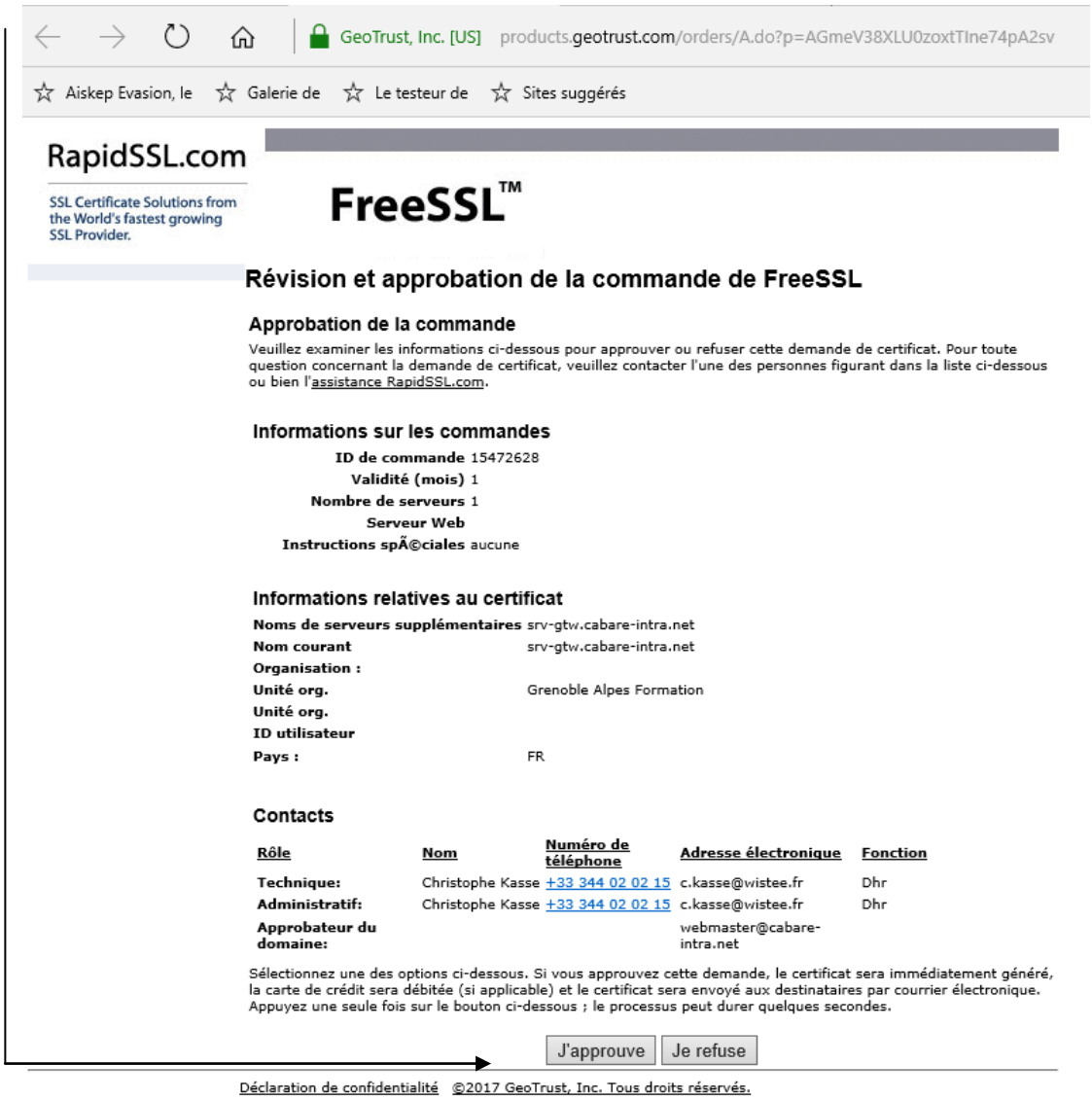
Informations du demandeur:

Nom: Christophe Kasse
E-mail: c.kasse@wistee.fr
Tel: +33 344 02 02 15

Nous vous invitons à cliquer sur l'URL ci-dessous pour revoir et approuver la demande de certificat.

https://products.geotrust.com/orders/A.do?p=AGmeV38XLU0zoxtTIne74pA2sv

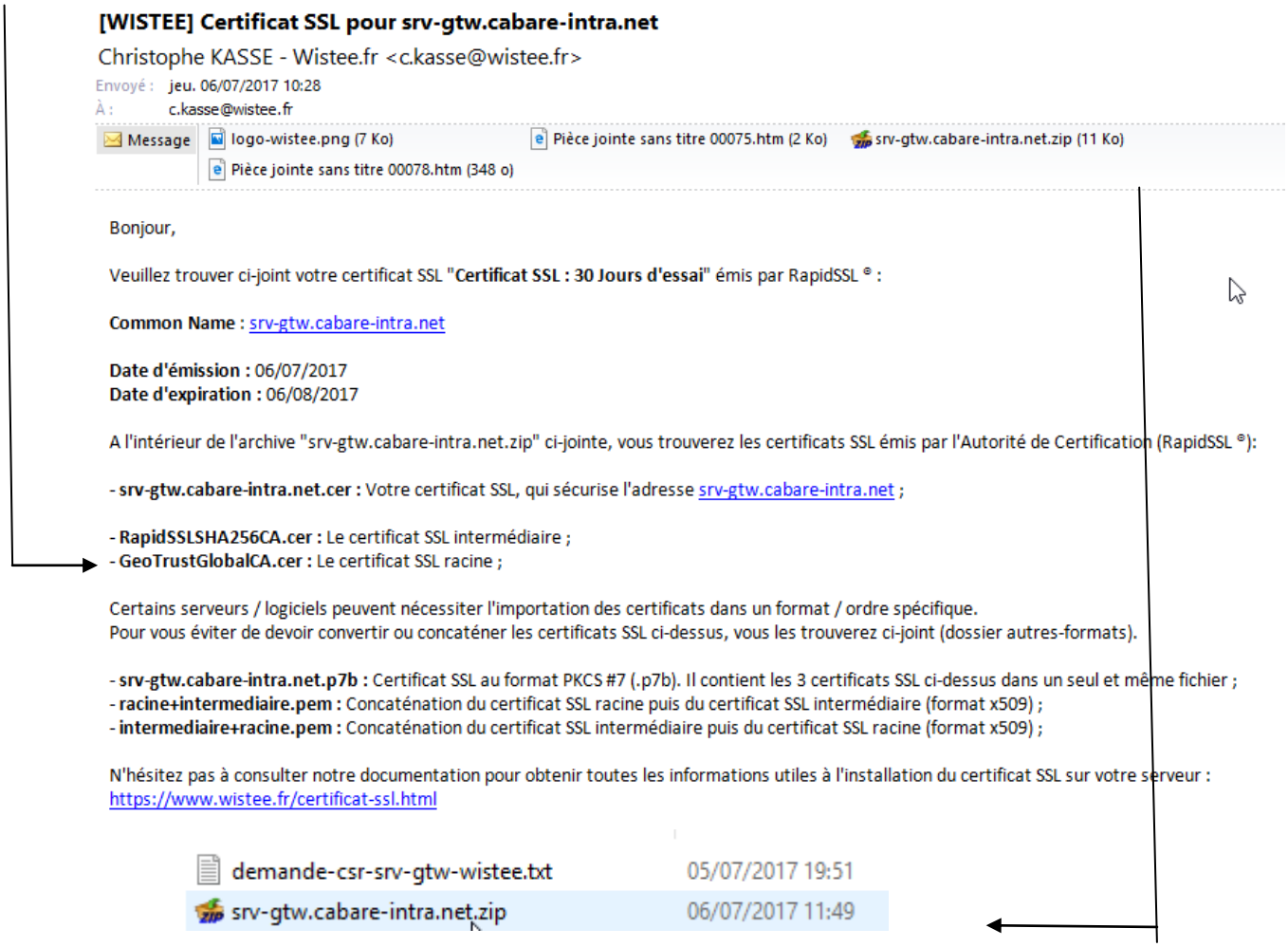
Dans lequel on doit vérifer l'exactitude des renseignements, et **approuver**



On a un quitus d'approbation

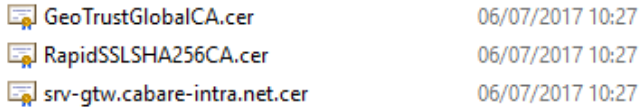
Réception des certificats émis par WISTEE

Wistee va envoyer dans les 24-48h un mail avec en pièce jointe le certificat de la part du CA, qui peut bien sur varier(**Trustprovider, geoTrustGlobalCa**…)

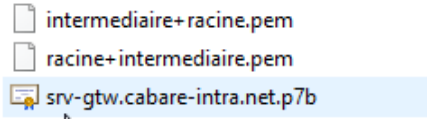


On a dedans effectivement pas mal de choses :

Nos 3 certificats **.cer** cités



Et aussi notre certificat SSL au format **PKCS#7**



Installation du certificat PKCS#7 Sur le Serveur Windows

N.B: Il faut préalablement avoir généré la requête **CSR** sur **IIS** afin que la clé privée soit présente sur le serveur.

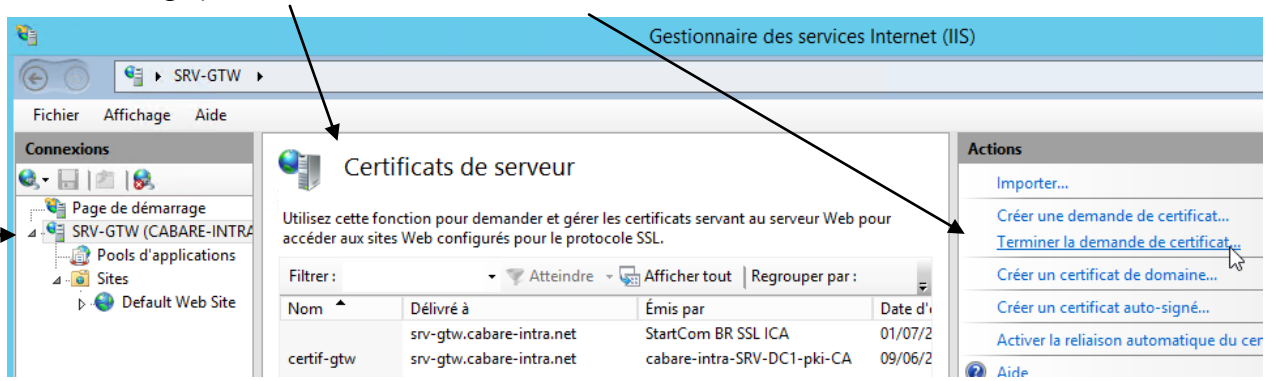
N.B: Si la requête **CSR** a été générée sur un autre serveur (Windows ou Linux), il faut importer le certificat au format **PKCS #12 (.pfx)** dans IIS

Par défaut, un **certificat SSL** est émis par **l'Autorité de Certification** au format **x509 (extension : .cer).**

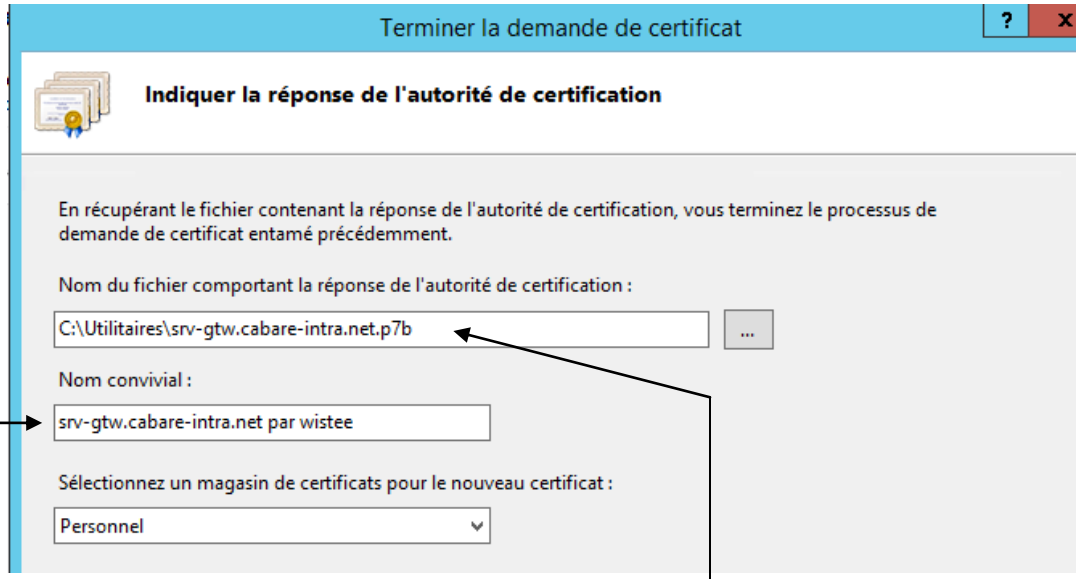
Chez **Wistee**, en plus du certificat au format **x509**, est envoyé aussi le certificat **SSL** déjà convertit au format **PKCS #7 (.p7b**).

Terminer la demande depuis Windows Internet Server

Sur **IIS**, on se place sur le serveur, on demande **Certificats de serveur**, puis on fait alors logiquement **Terminer la demande de certificat**



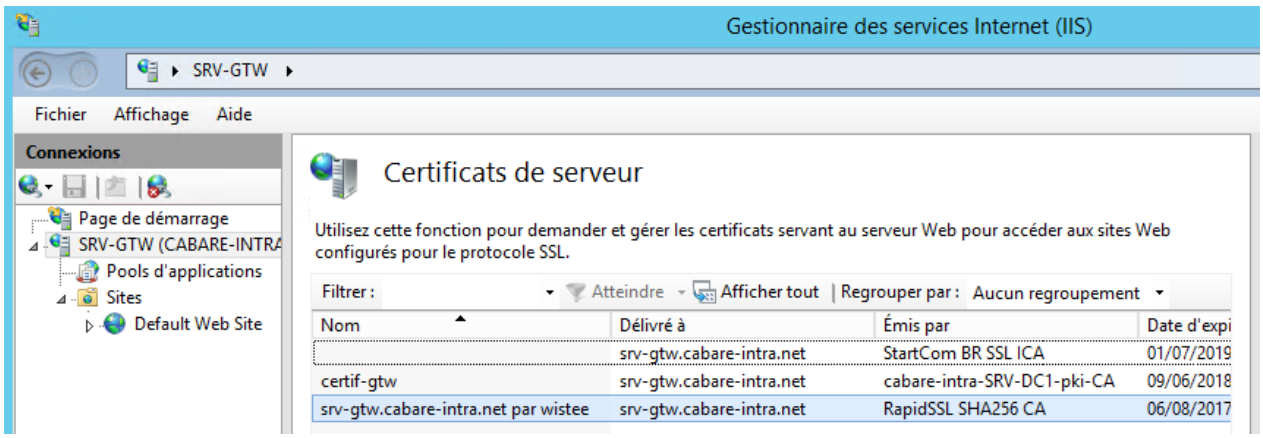
On obtient



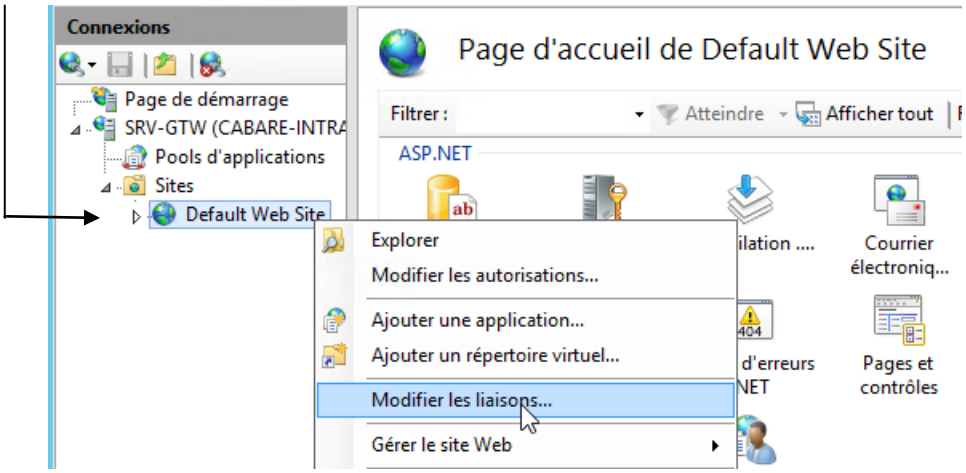
Par défaut, seuls les fichiers **".cer**" sont listés, il faut sélectionner donc *.* pour sélectionner le certificat SSL au format "P7B / PKCS#7".

On donne un nom "parlant" au certificat, pour s'y retrouver ensuite

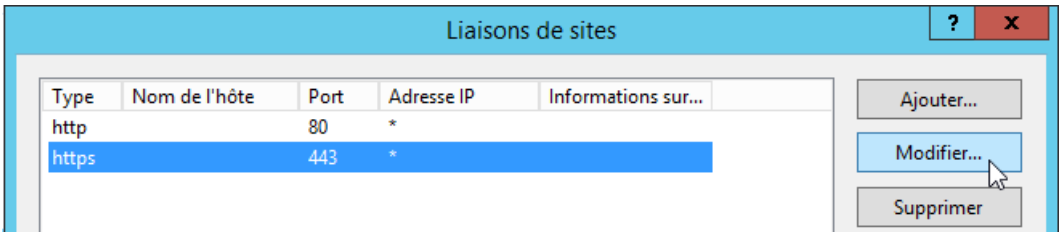
et on devrait obtenir



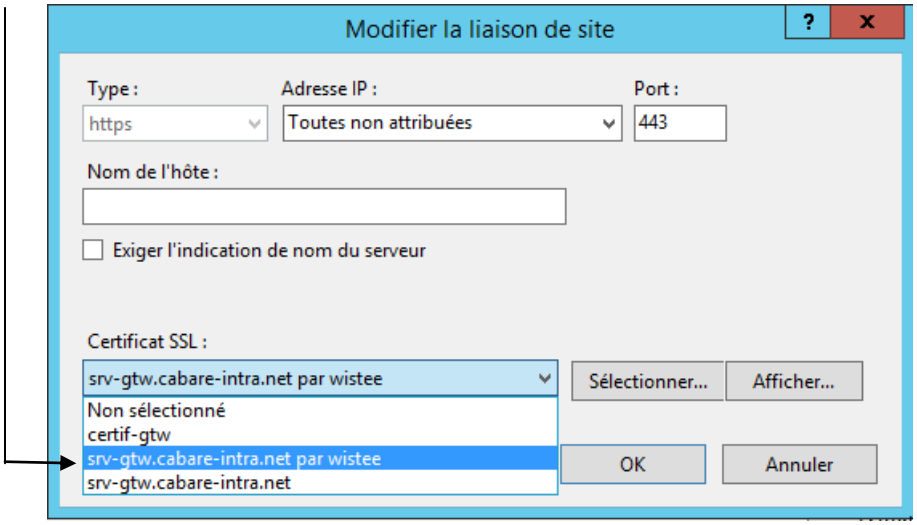
Il faut assigner le certificat à la liaison https:443, via le **site web par défaut**, puis clic droit **Modifier les liaisons**



On choisit 443 et on demande **Modifier**



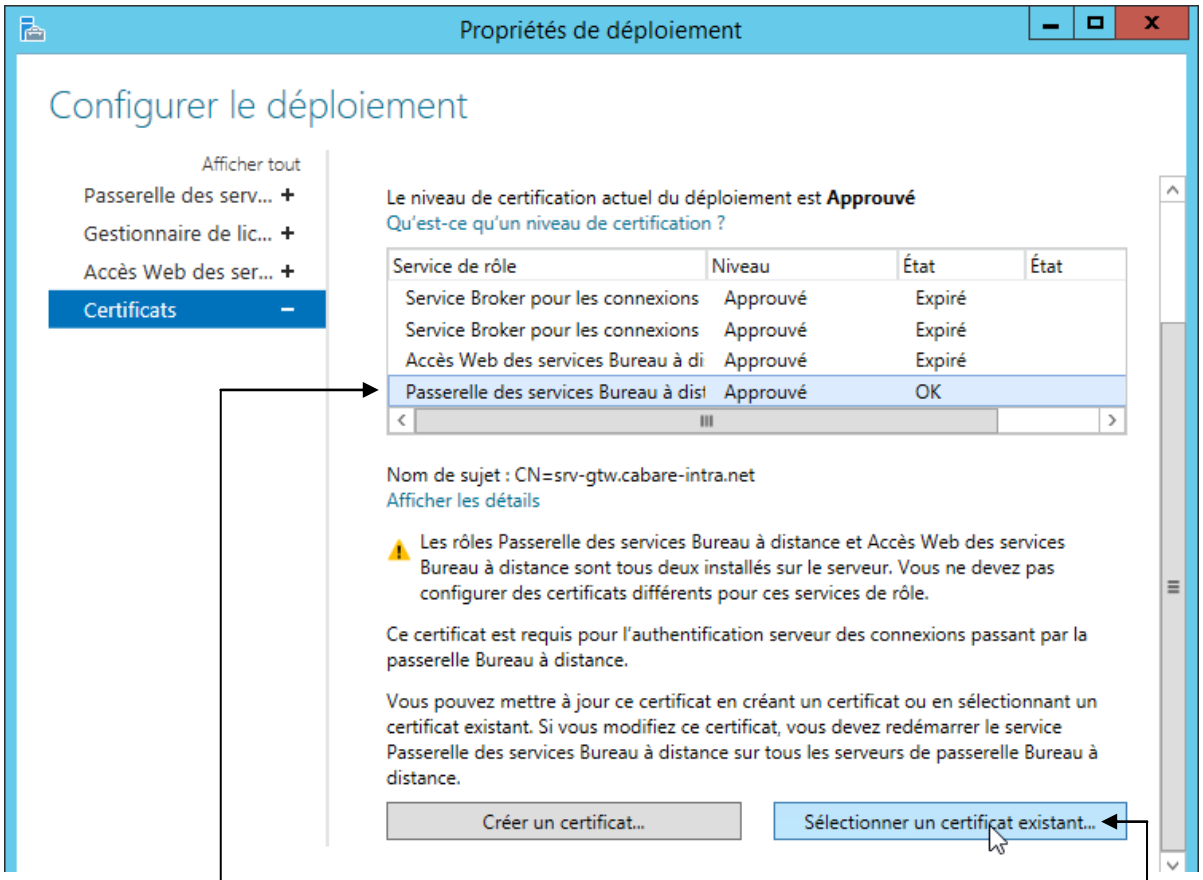
Et on choisit notre certificat avec son nom "parlant"



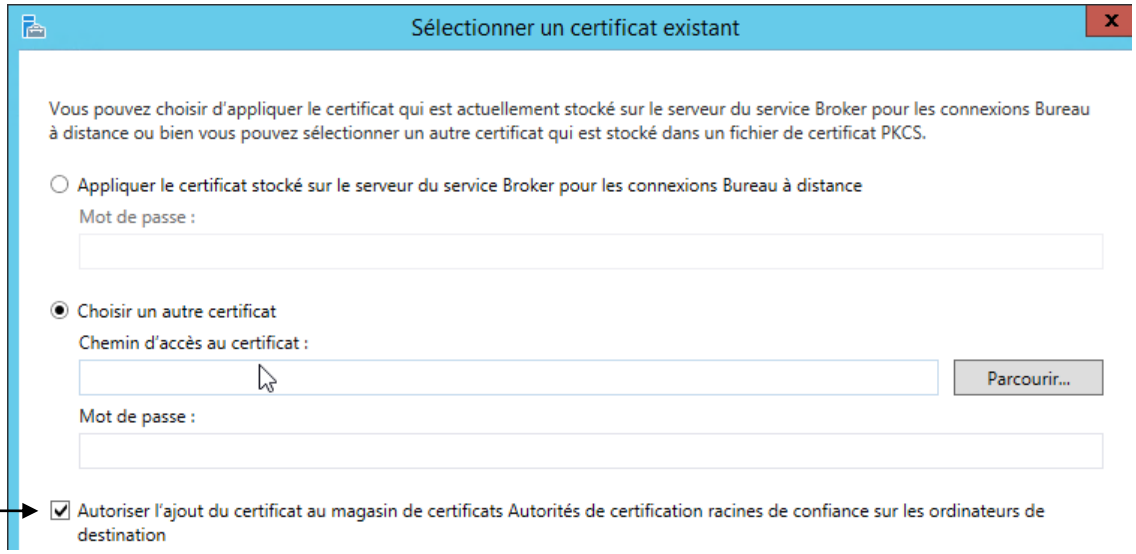
INSERER UN CERTIFICAT DANS RDS

A partir de certificat pfx (ou p12):

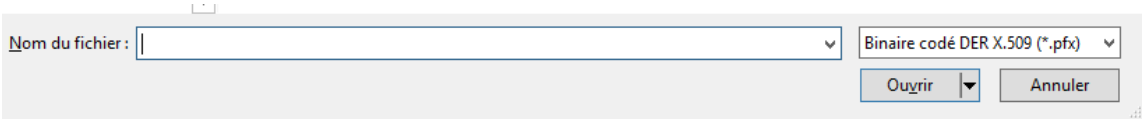
Une fois sur le serveur RDS qui permet l'accès à la console **Services à distance**,



On pointe le certificat à mettre à jour, (par exemple la passerelle) Puis on demande **Sélectionner un certificat existant**…



Lorsque l'on demande **ajouter un certificat**, on ne peut ajouter ici que des certificats au format **DER X509 (.pfx)**


Nom du fichier :
Binaire codé DER X.509 (*.pfx)
Ouvrir
Annuler

CERTIFICAT GANDI SUR INSTANCE SIMPLE HOSTING

Demande de certificat CSR – via Linux Gandi (console SSH) CSRL

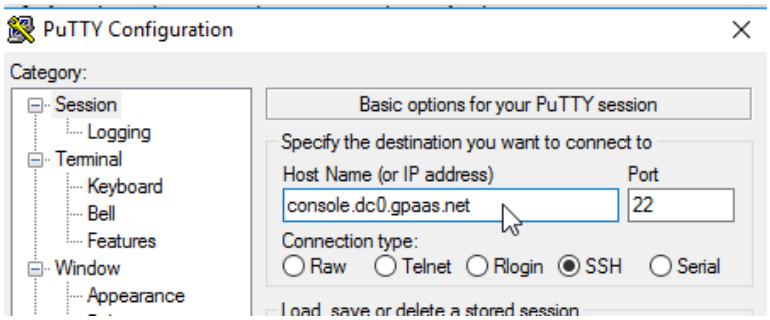
On peut faire la demande **CSR** depuis le serveur **Gandi Simple Hosting** sur lequel on souhaite installer le certificat à travers une **console SSH** (permettant ensuite de passer la commande OpenSSL, mais aussi toutes les commandes souhaitées d'ailleurs)

On a alors dans les "mains 2 fichiers, la **clé Privée** au format **.key** (associée à un mot de passe) et un fichier "public" **.cer** qui contient notre identification et notre demande de certificat, qu'il faudra envoyer à l'autorité de Certification.

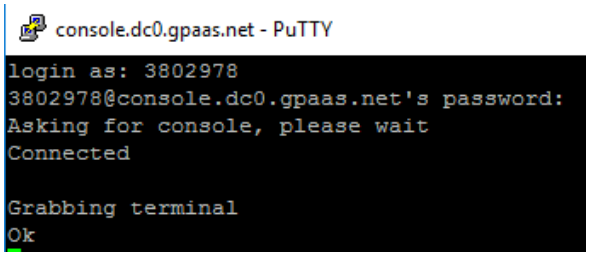
Lancement console SSH

Une fois activée la console **SSH** dans l'interface d'administration **GANDI** pour **l'instance** voulue, par exemple ***milo*** (Cf **annexe 2**)

Il faut lancer la console **Putty** et prendre la connexion sur l'instance ***milo*** avec **console.dc0.gpaas.net** comme adresse de la machine a atteindre

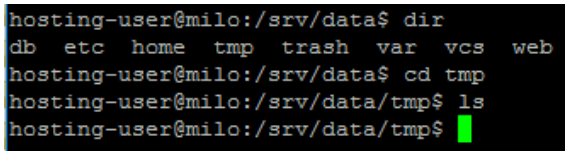


et pour milo ce sera login ***3802978*** mdp ***Gandimilozk28***



Placement en Invite de Comande

Pour pouvoir passer les commandes OPENSSL voulue il faut d'abord se placer dans le dossier **srv/data/tmp**



Commande OPENSSL

La syntaxe de la commande est

openssl req -newkey rsa:2048 -nodes -sha256 -keyout *www.votre-domaine.fr.key* -out *www.votre-domaine.fr.csr*

```
hosting-user@milo:/srv/data/tmp$ openssl req -newkey rsa:2048 -nodes -sha256 -ke
yout www.cabare-formation.fr.key -out www.cabare-formation.fr.csr
```

Cette commande va déclencher plusieurs invites auxquelles il va falloir répondre :

```
Generating a 2048 bit RSA private key
.....................................+++
.....................................................................................
.....................+++
writing new private key to 'www.cabare-formation.fr.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) [AU]:
```

Country Name (2 letter code) : il s'agit du code pays (Exemple : FR)

```
State or Province Name (full name) [Some-State]:ISERE
```

State or Province Name (full name) : le département

```
Locality Name (eg, city) []:FONTAINE
```

Locality Name (eg, city) : la ville

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Grenoble Alpes Format
ion
```

Organization Name (eg, company)

Pour les particuliers : nom et prénom

Pour les professionnels : la raison sociale telle qu'elle apparait sur Infogreffe (obligatoire)

```
Organizational Unit Name (eg, section) []
```

Organizational Unit (eg, section) : optionnel

```
Common Name (e.g. server FQDN or YOUR name) []:www.cabare-formation.fr
```

Common Name (eg, server FQDN or YOUR name)

On indique "www.votre-domaine.fr" ce qui sécurisera également "votre-domaine.fr".

> **N.B**: Si on vous renseigne "votre-domaine.fr", l'adresse "www.votre-domaine.fr" ne sera pas sécurisée.
>
> **N.B**: Certificat SSL Wildcard : Renseignez : *.votre-domaine.fr en tant que Common Name, (a déconseiller !)

```
Email Address []:
```

Email Address : optionnel

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

optionnel

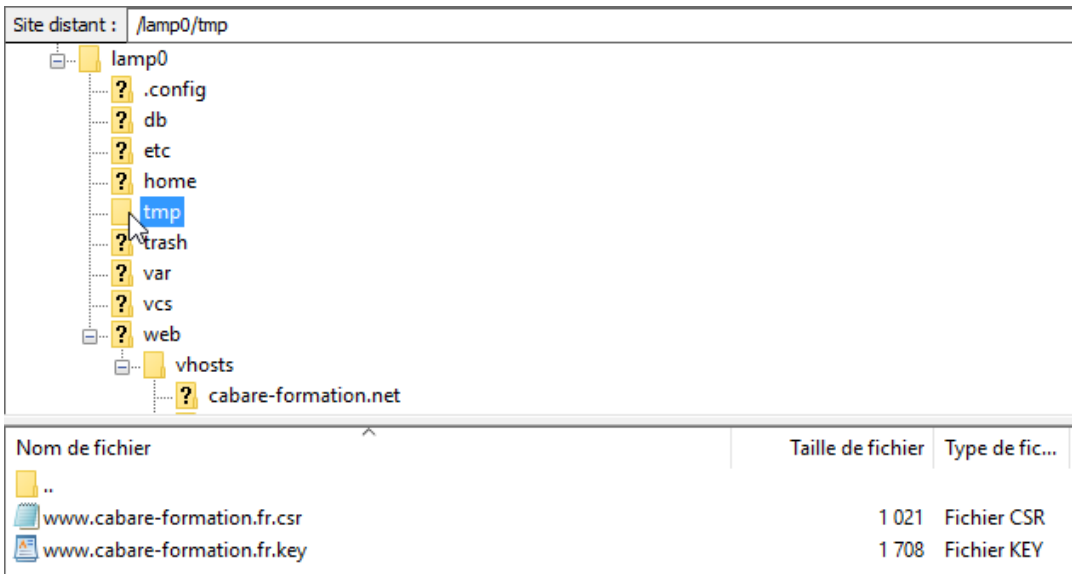
```
An optional company name []:
```

Optionnel

A la fin de la commande on obtient 2 fichiers, crées avec le nom de domaine à protéger, la **CSR** en **.csr** et la **clé privée** en **.key.** Que l'on peut voir par **ls**

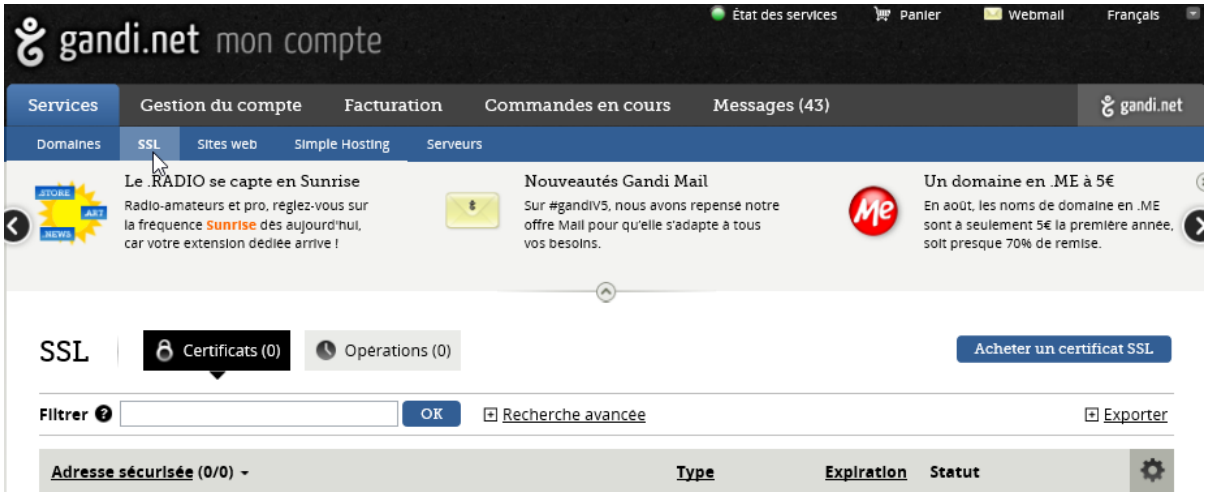
```
hosting-user@milo:/srv/data/tmp$ ls
www.cabare-formation.fr.csr  www.cabare-formation.fr.key
```

On retrouve bien sur ces 2 fichiers dans notre instance, accessibles via SFTP dans le dossier tmp

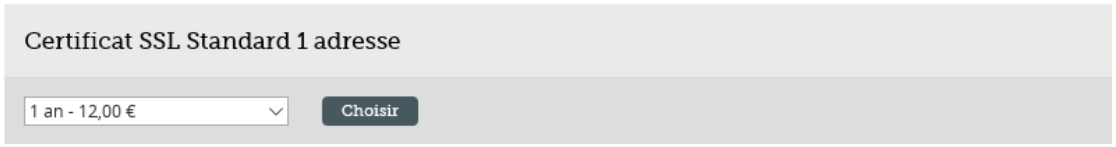


Envois Demande de certificat CSR via site web Gandi

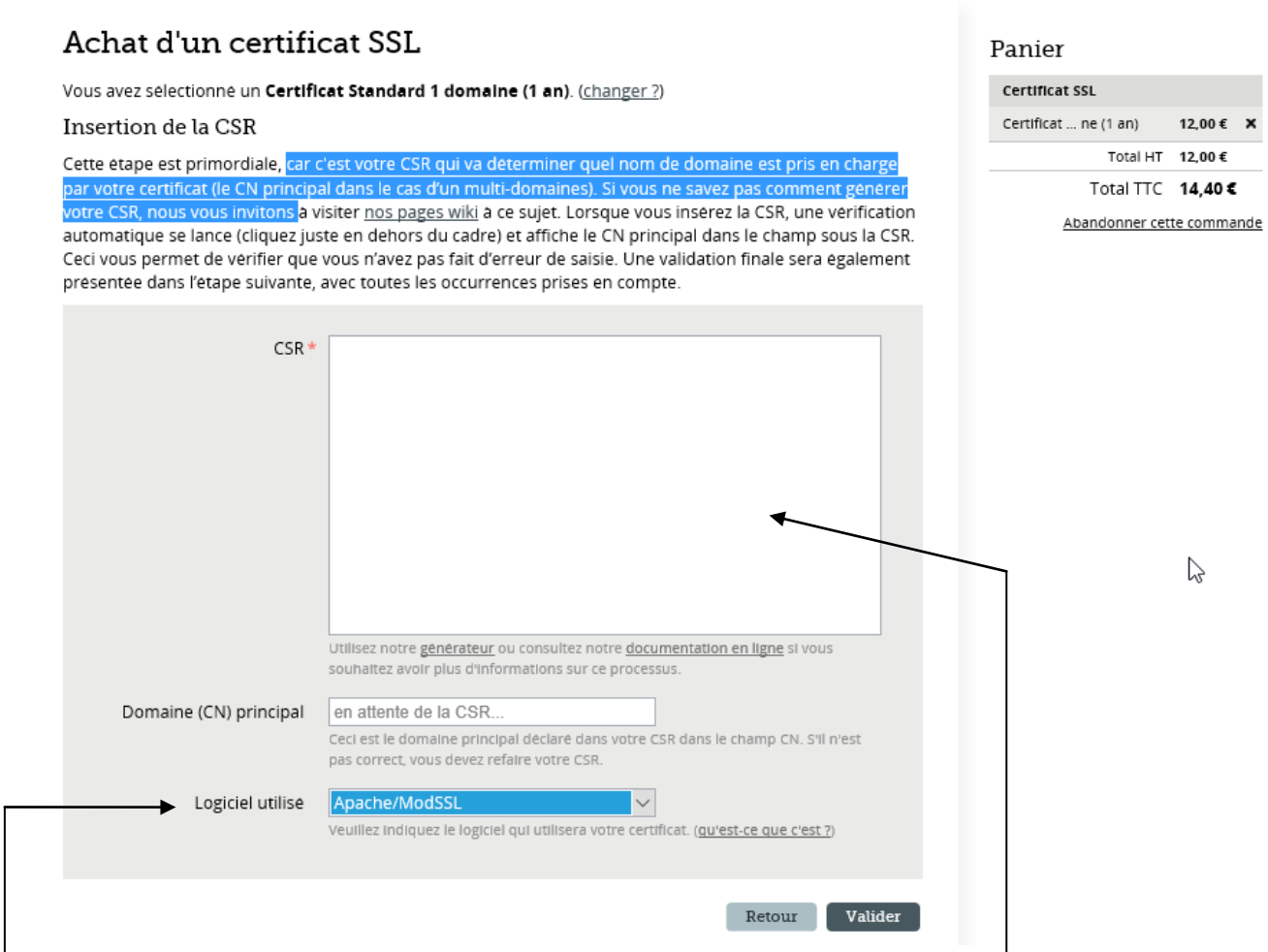
Il faut envoyer la **demande de certificat CSR** par l'interface **GANDI** onglet **SSL** puis **Acheter un certificat SSL**



Le **certificat SSL standard** suffirait



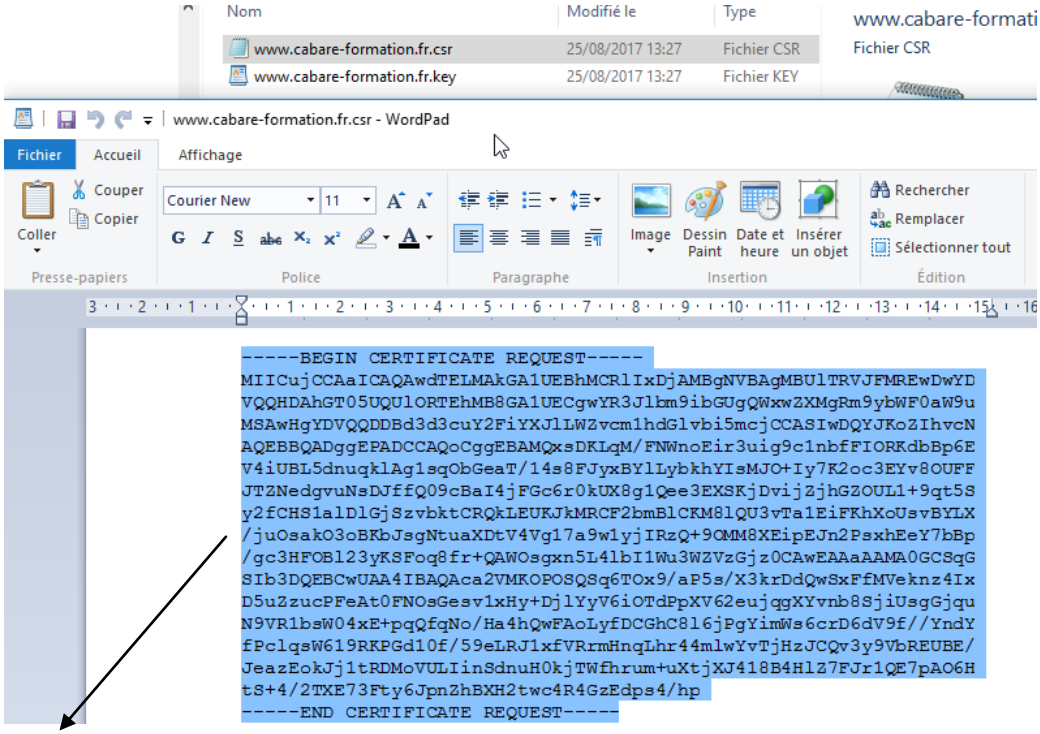
Et l'on obtient



Dans cette fenêtre il va falloir alors :

- Copier coller la demande CSR obtenu via la commande OPENSSL effectuée précédamment
- Vérifier que le nom de domaine qui apparaît soit le bon
- Spécifier que la CSR a été effectuée sur Apache/modSSL

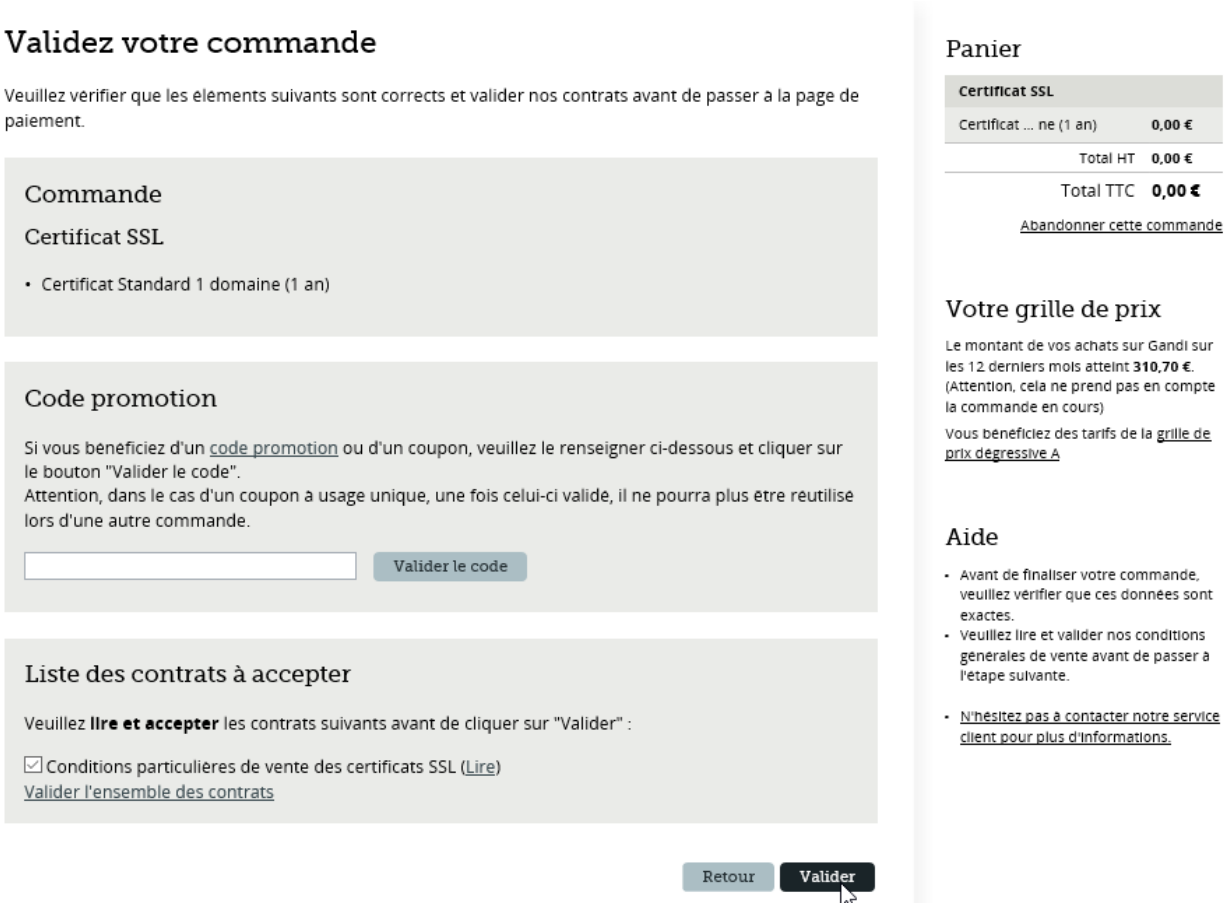
Pour faire un copier coller de la demande CSR il faut ouvrir le fichier .csr obtenu précédemment pra la commande OPENSSL…



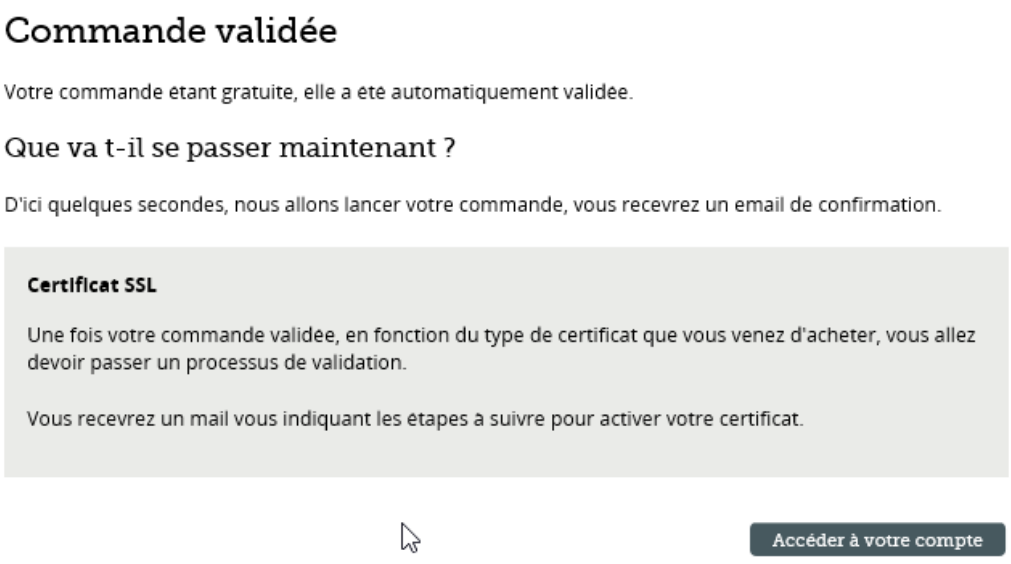
On le colle ici

On vérifie le nom de domaine, on spécifie **Apache/ModSSL** puis V**alider**

On annonce le tarif à 0 car on dispose de 1 certificat gratuit par domaine la 1° année.



Et la commande de certificat est passée!



Traitement Demande de certificat par Gandi

Gandi va instancier la demande de certificat, et on doit valider l'appartenance/propriété du domaine via un mail de confirmation (exemple)

De : Gandi <support-fr@support.gandi.net>
À : michel@cabare.net
Cc :
Objet : [GANDI] Achat d'un certificat SSL Standard pour le domaine www.cabare-formation.fr

Bonjour,

Vous avez acheté un certificat SSL Standard pour le(s) domaine(s) suivant(s) :
www.cabare-formation.fr

Afin de pouvoir vérifier que votre adresse email est valide (notamment pour la suite de la procédure), merci de cliquer sur le lien ci-dessous :
https://www.gandi.net/admin/contact/validate/68bfb18b06950f44fc173919f1cc351dd6e17925
(si votre navigateur ne permet pas l'ouverture par clic direct, merci de copier l'intégralité du lien et de le coller dans la barre d'adresse de votre navigateur).
Une fois cette étape terminée, le process de validation du certificat pourra continuer.

N'hésitez pas à contacter notre service client en cas de problème ou pour toute autre question : http://www.gandi.net/faq/contact_support

Nous vous remercions de votre confiance.

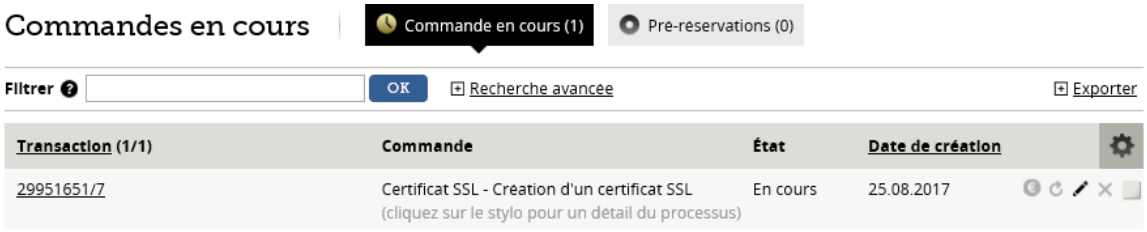
Cordialement.

Dans lequel on doit valider l'exactitude des renseignements,

Validation du contact

Le contact **michel cabaré** sur l'adresse email **michel@cabare.net** est maintenant un contact valide
Vous pouvez passer à l'etape suivante.

et cela déclanche la commade de certificat



Commandes en cours | Commande en cours (1) | Pre-réservations (0)

Filtrer | OK | Recherche avancée | Exporter

Transaction (1/1)	Commande	État	Date de création
29951651/7	Certificat SSL - Creation d'un certificat SSL (cliquez sur le stylo pour un detail du processus)	En cours	25.08.2017

Si le domaine n'est pas chez gandi, on peut choisir entre 3 options de validation, (email / DNS / fichier TXT) (chez gandi l'option DNS est effectuée automatiquement)

Bonjour,

Ceci est un email automatique vous informant que la procédure de validation de votre certificat SSL Standard est commencée.
Afin de suivre celle-ci et pouvoir réaliser les actions de vérification, nous vous invitons à vous connecter (avec votre identifiant MC1557-GANDI) sur cette interface :
https://www.gandi.net/admin/ssl/steps/96147446

Pour rappel, selon la méthode de validation que vous avez choisi, il vous est demandé :

pour une validation par email
de créer l'adresse email de contact admin@cabare-formation.fr (ainsi que pour chaque autre domaine dans le cas d'un certificat multi-domaines) afin de recevoir le message de vérification (lien inclus à cliquer). Attention : si vous avez tardé à créer cette adresse, vous avez peut-être déjà raté celui-ci : vous pouvez alors via l'interface, relancer l'envoi.

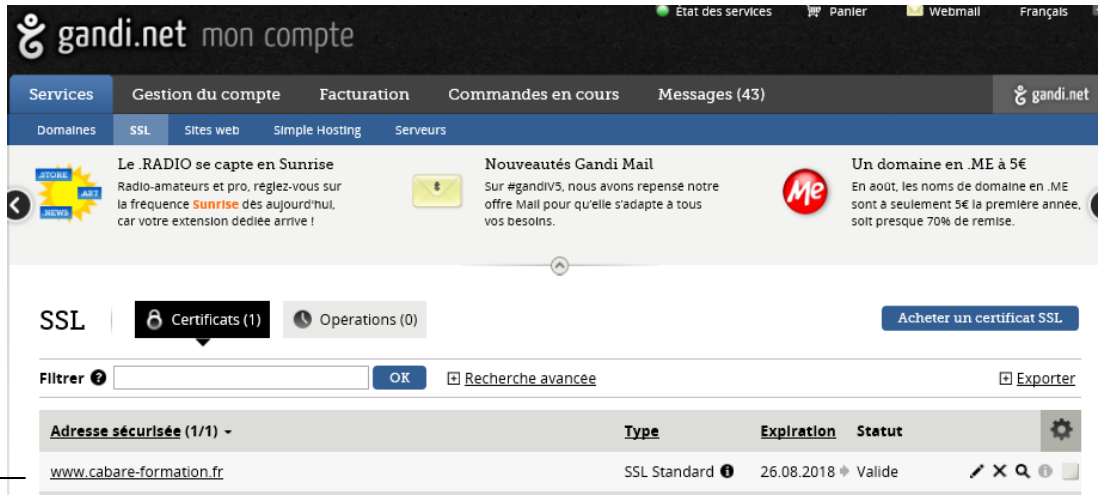
pour une validation par DNS
de modifier la zone DNS de cabare-formation.fr en ajoutant l'enregistrement CNAME qui est communiqué sur l'interface. En cas de certificat Multi-domaines, cette opération est à réaliser pour chaque nom de domaine.

pour une validation par fichier
de récupérer le fichier .TXT sur l'interface (lien 'récupérer') et de copier celui-ci à la racine du répertoire contenant le site web sur lequel pointe le nom de domaine à certifier. En cas de certificat Multi-domaines, cette opération est à réaliser pour chaque nom de domaine.

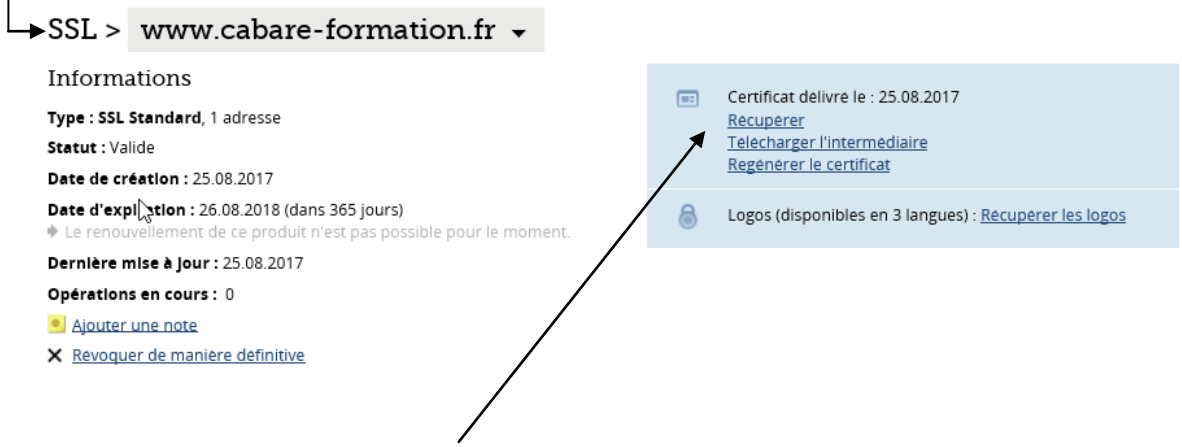
Si vous n'avez pas eu à choisir entre ces 3 méthodes, c'est que votre nom de domaine est chez Gandi et que vous avez les droits sur celui-ci. La méthode de validation par DNS a donc été automatiquement choisie et configurée. Cette étape se validera donc prochainement.

Réception des certificats émis par Gandi

Les certificats crées **Gandi** sont listés sur l'interface, dans l'onglet **SSL**



Lorsque l'on clique dessus, on obtient le détail



Il faut maintenant récupérer le certificat afin de l'installer sur le serveur. On demande simplement "**Récupérer**" : Le certificat crypté s'affiche dans une fenêtre appelée "**Visualisation du certificat**" :

Cette fenêtre permet

- soit de copier manuellement le certificat crypté à coller dans un fichier texte au format **.crt**

-----BEGIN CERTIFICATE-----

....texte crypté...

-----END CERTIFICATE-----

- soit de télécharger le certificat + si besoin le certificat intermédiaire !

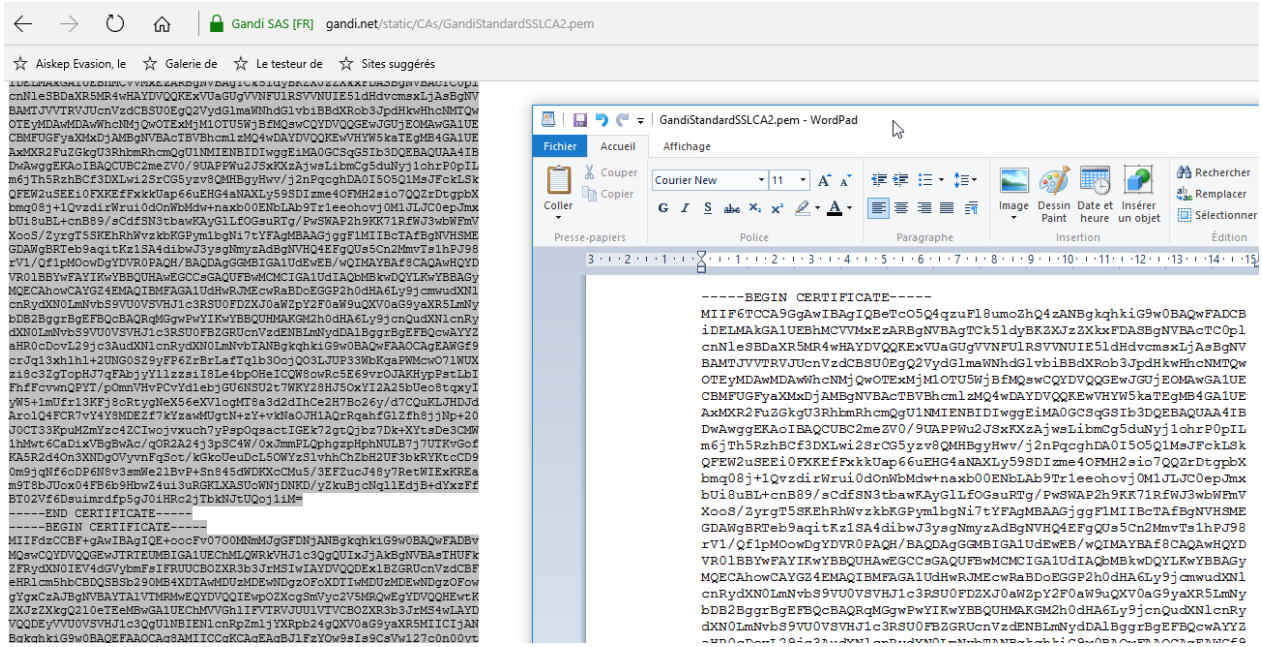
on peut donc récupérer le certificat par copier / coller dans un fichier texte

www.cabare-formation.fr.crt - Bloc-notes

Fichier Edition Format Affichage ?

```
-----BEGIN CERTIFICATE-----
MIIFDTCCA/WgAwIBAgIRALVINtdVBIAKX8URqCxHG+owDQYJKoZIhvcNAQELBQAw
XzELMAkGA1UEBhMCRlIxDjAMBgNVBAgTBVBhcmlzMQ4wDAYDVQQHEwVQYXJpczEO
MAwGA1UEChMFR2FuZGkxIDAeBgNVBAMTF0dhbmRpIFN0YW5kYXJkIFNTTCBDQSAy
MB4XDTE3MDgyNTAwMDAwMFoXDTE4MDgyNTIzNTk1OVowYjEhMB8GA1UECxMYRG9t
YWluIENvbnRyb2wgVmFsaWRhdGVkMRswGQYDVQQLExJHYW5kaSBTdGFuZGFyZCBT
U0wxIDAeBgNVBAMTF3d3dy5jYWJhcmUtZm9ybWF0aW9uLmZyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxDGwMouoz8U1aegSKve6KD1zWdt8Ug5Ep1sG
noRXiJQEvl2e6qSUCDWyo5sZ5pP/XizwUnLEFiUvJuSFgiwwk74jLsrahzcRi/w5
QUUlNk152C+42wMl99DT1wFojiMUZzqvSRRfyDVB57cRdIqMO+KNmOEZk5QvX72q
3lLLZ8IdLVqUOUaNLO9uS0JFCQsRQomQxEIXZuYGUIozyVBTe9NrUSIUqFehSy8F
gtf+O46xqQ7egEpsmyA225pcO1XhWDXtr3DXKMhHND704wzxcSKkQmfY+zGER5jt
sGn+BzccU4GXbfIpIWirx+v5ABY6yDGfkviVsjVa7dZ1XMaPPQIDAQABo4IBvzCC
AbswHwYDVR0jBBgwFoAUs5Cn2MmvTs1hPJ98rV1/Qf1pMOowHQYDVR0OBBYEFB4/
fK6TNiucaAIuLpbxu5tBKuvmMA4GA1UdDwEB/wQEAwIFoDAMBgNVHRMBAf8EAjAA
MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjBLBgNVHSAERDBCMDYGCysG
AQQBsjEBAgIaMCcwJQYIKwYBBQUHAgEWGWh0dHBzOi8vY3BzLnVzZXJ0cnVzdC5j
b20wCAYGZ4EMAQIBMEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHA6Ly9jcmwudXNlcnRy
dXN0LmNvbS9HYW5kaVN0YW5kYXJkU1NMQ0EyLmNybDBzBggrBgEFBQcBAQRnMGUw
PAYIKwYBBQUHMAKGMGh0dHA6Ly9jcnQudXNlcnRydXN0LmNvbS9HYW5kaVN0YW5k
YXJkU1NMQ0EyLmNydDAlBggrBgEFBQcwAYYZaHR0cDovL29jc3AudXNlcnRydXN0
LmNvbTA3BgNVHREEMDAughd3d3cuY2FiYXJlLWZvcm1hdGlvbi5mcoITY2FiYXJl
LWZvcm1hdGlvbi5mcjANBgkqhkiG9w0BAQsFAAOCAQEAfFJY8FaEOvC0pSqXkynY
r8OLKP2NmG9y5OT3/1biAN5Rf+Ob09swu8YS+QAp3FmpUubSIU1+1Wd4+iXEWX2e
Lh01G54C0oZrMgUdwctxfDsj7RJOcsWJRiDB7tKdkfJ0Pvj+iRuW1wrMSFp9M81O
JMp/BlQXVGkqdi3TzdXvEM2Cz693ptdBTuuTxSBDH9TUYMlj3vNHrSL3zJaJX/bo
FMRRyP4hvQCJO3xQ4j3AtSJ4McJjuGHSoM2qvdVWvquUg8EisVviHmzRb/Cv8jLp
7hN73DdZcG03OLq34UJkIRTwL6adIAeWEx3oabp67GP8hxPxKIfbgy+EILH0/VHp
Sw==
-----END CERTIFICATE-----
```

On peut aussi télécharger le certificat et le certificat intermediaire par l'interface !!!

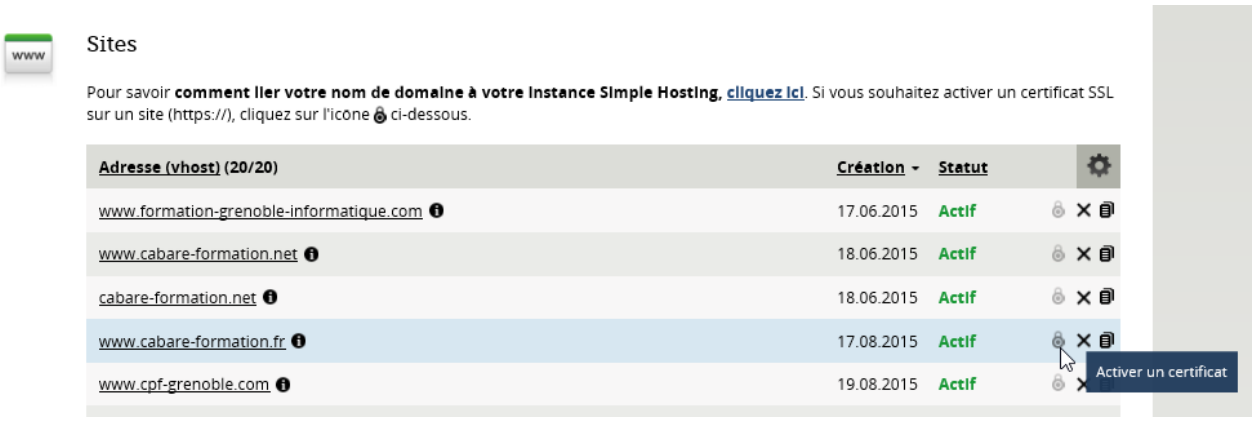


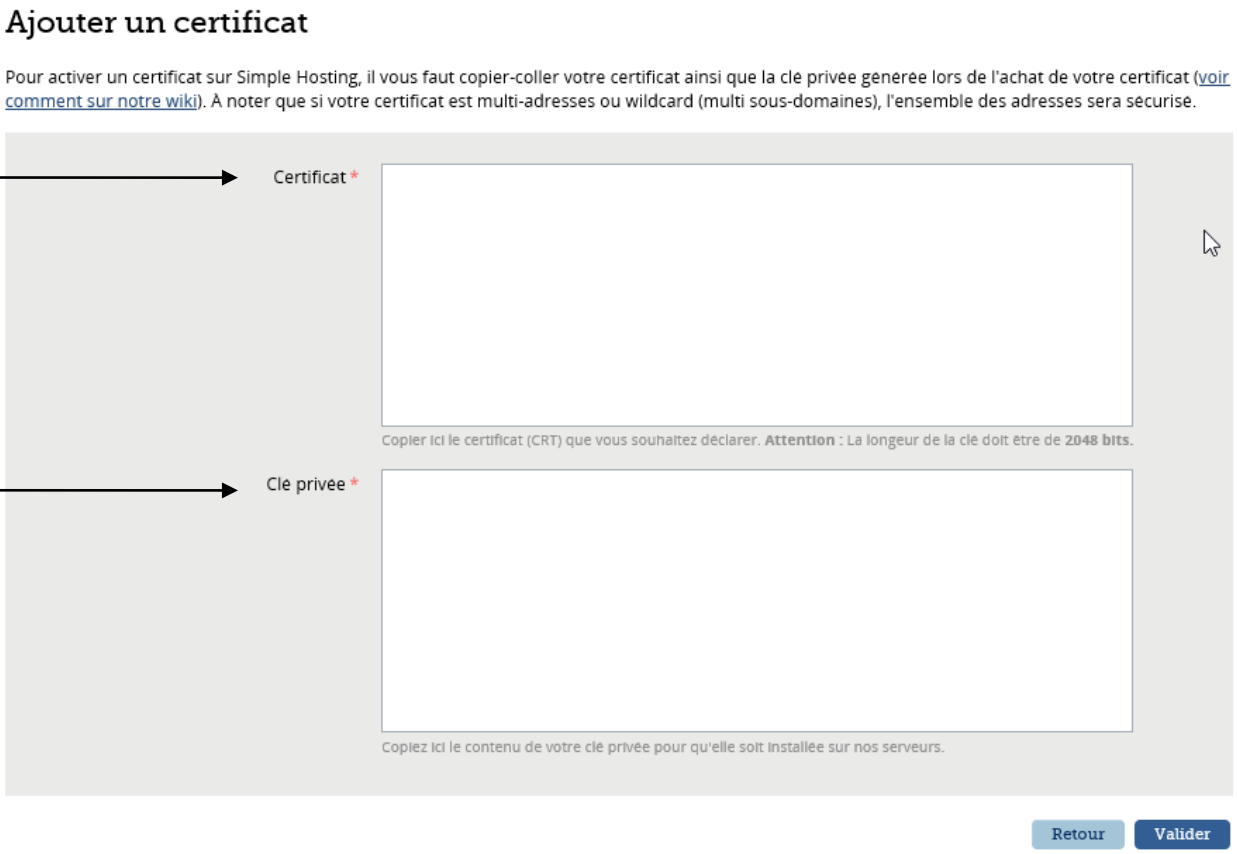
Installation du certificat sur le serveur Linux Simple Hosting

Une fois en possession au minimum

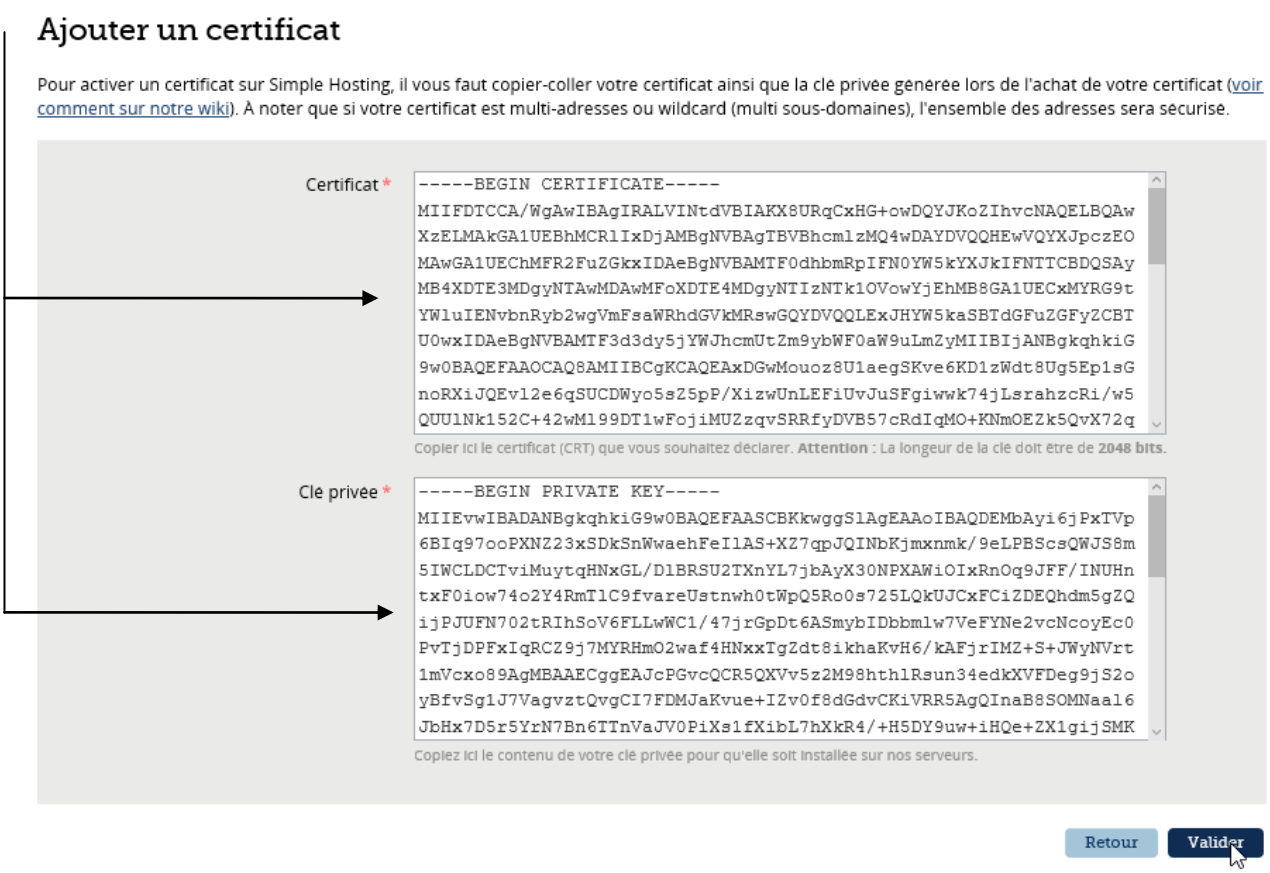
- De la clé privée
- Du certificat SSL

On peut installer le certificat sur notre instance **Simple Hosting**

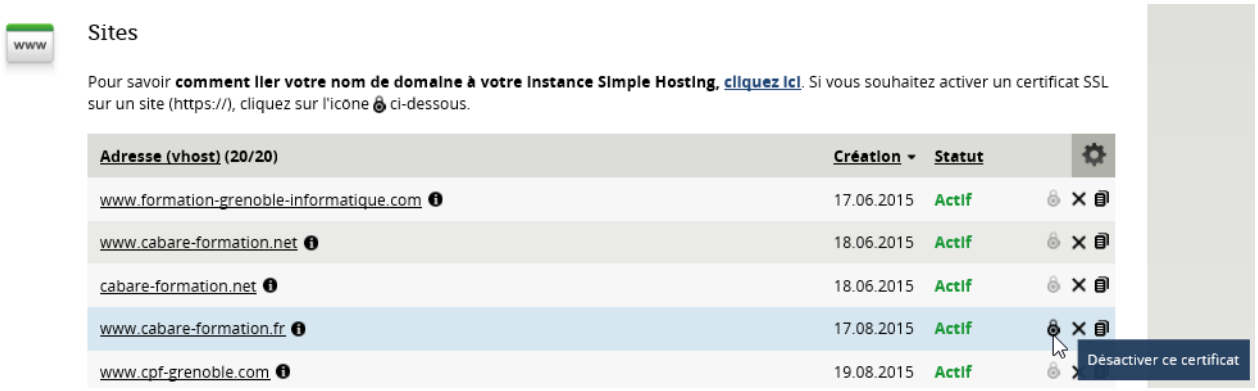




Une fois copier / coller le contenu du certificat et de la clé, on peut **valider**



Désormais le certificat est activé :



Certificat intermédiaire, ou non

N.B: Téléchargement du certificat intermédiaire

Le certificat intermédiaire Gandi est différent pour un certificat de la gamme Standard et un certificat de la gamme Pro ou encore de la gamme Business.

Ce certificat intermédiaire devra ensuite être installé sur le serveur hébergeant le site répondant à l'adresse protégé, de la même façon que le certificat qui vous a été délivré

Forcer https sur Simple Hosting avec .htaccess (base)

Lorsqu'un **certificat SSL** est installé sur votre instance **Simple Hosting**, il est possible d'augmenter la sécurité du site en forçant l'accès via **https**.

Pour rediriger **http://** vers **https://.**

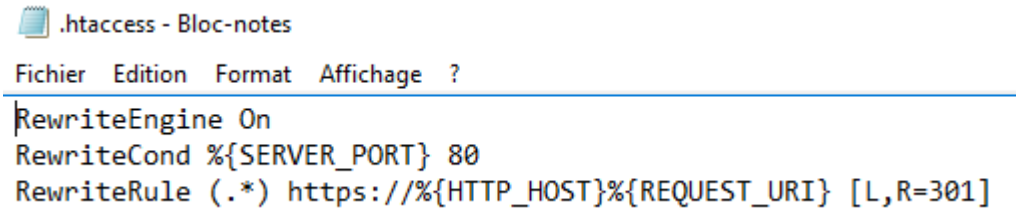
- Le fichier **.htaccess** doit être placé dans le dossier "**htdocs**" du site vhost sur lequel on souhaite utiliser https.

On force donc l'utilisation de HTTPS avec un fichier .htaccess contenant :

RewriteEngine on

RewriteCond %{SERVER_PORT} 80

RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]



Redirection http + https de domaine sur www.domaine (complet)

On ne veut plus rediriger simplement **http://** vers **https://.**

Mais aussi les Url avec ou sans www

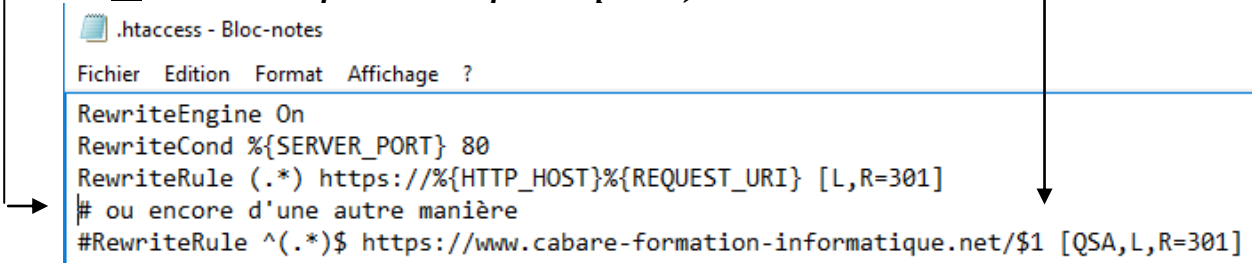
Donc si on déclare www.mondomaine.com, il faut penser à ajouter 3 redirections de type 301

de http://***mondomaine.com*** vers	https://***www.mondomaine.com***.
de http://***www.mondomaine.com*** vers	https://***www.mondomaine.com***.
de https://***mondomaine.com*** vers	https://***www.mondomaine.com***.

On utilisera 2 fichiers htacces, respectivement sur le host principal en www et sur un 2° host crée sans www. (NB: ^=debut $=fin !=different)

Sur le **host principal en www** on met un fichier **.htaccess** permettant par exemple la

- redirection des http sur le port 80 sur les https (ou d'une autre manière sur https de ***www.cabare-formation-informatique.net)***



Sur le **2° host nommé sans les www**, on met un fichier **.htaccess** permettant par exemple la

- redirection de http de ***cabare-formation.net*** (tout ce qui n'est pas www.cabare-formation-iformatique.net) vers httpS de ***www.cabare-formation-informatique.net***

.htaccess - Bloc-notes

Fichier Edition Format Affichage ?

```
RewriteEngine On
RewriteBase /
RewriteCond %{HTTP_HOST} !^www.cabare-formation-informatique.net$ [NC]
RewriteRule ^(.*)$ https://www.cabare-formation-informatique.net/$1 [L,R=301]
```

Logo validation https sur Simple Hosting avec certificat standard

Lorsqu'un **certificat SSL** est installé sur votre instance **Simple Hosting**, il est possible de mettre un lien sur une image (un peu comme la validation Htp5 ou css3 auprès du W3c)

On récupère le lien au niveau de l'interface Gandi au même endroit où l'on récupère les certificats, via **Récupérer les logos**

SSL > www.cabare-formation.fr

Informations

Type : SSL Standard, 1 adresse

Statut : Valide

Date de création : 25.08.2017

Date d'expiration : 26.08.2018 (dans 356 jours)

Le renouvellement de ce produit n'est pas possible pour le moment.

Dernière mise à jour : 25.08.2017

Certificat délivré le : 25.08.2017
Récupérer
Télécharger l'intermédiaire
Regénérer le certificat

Logos (disponibles en 3 langues) : Récupérer les logos

Récupération des logos

Vous pouvez récupérer les logos ci-dessous (format .png) en cliquant dessus avec le bouton droit et en choisissant "Enregistrer l'image sous...". Vous disposez des logos en version française, anglaise et espagnole.

Lien de vérification du certificat :

- www.cabare-formation.fr : https://www.gandi.net/ssl/secured/www.cabare-formation.fr/493865/84ad148253

sécurisé par gandi.net | secured by gandi.net | securizado por gandi.net

CERTIFICAT WISTEE SUR INSTANCE GANDI SIMPLE HOSTING

Demande de certificat CSR – via Linux Gandi (console SSH) CSRL

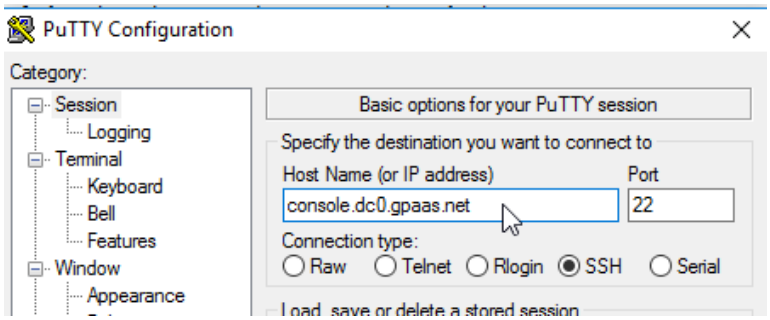
On doit faire la demande **CSR** depuis le serveur **Gandi Simple Hosting** sur lequel on souhaite installer le certificat à travers une **console SSH** (permettant ensuite de passer la commande OpenSSL, mais aussi toutes les commandes souhaitées d'ailleurs)

On a alors dans les "mains 2 fichiers, la **clé Privée** au format **.key** (associée à un mot de passe) et un fichier "public" **.cer** qui contient notre identification et notre demande de certificat, qu'il faudra envoyer à l'autorité de Certification.

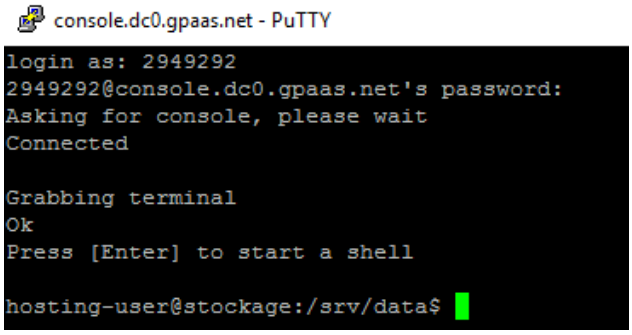
Lancement console SSH

Une fois activée la console **SSH** dans l'interface d'administration **GANDI** pour **l'instance** voulue, par exemple ***stockage*** (Cf **annexe 2**)

Il faut lancer la console **Putty** et prendre la connexion sur l'instance ***stockage*** avec **console.dc0.gpaas.net** comme adresse de la machine a atteindre

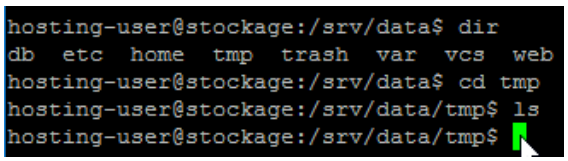


et pour stockage ce sera login ***2949292*** mdp ***Gandistockzk28***



Placement en Invite de Comande

Pour pouvoir passer les commandes OPENSSL voulue il faut d'abord se placer dans le dossier **srv/data/tmp**



Commande OPENSSL

La syntaxe de la commande est

openssl req -newkey rsa:2048 -nodes -sha256 -keyout *www.votre-domaine.fr.key* -out *www.votre-domaine.fr.csr*

```
hosting-user@stockage:/srv/data/tmp$ openssl req -newkey rsa:2048 -nodes -sha256
 -keyout www.cabare.net.key -out www.cabare.net.csr
```

Cette commande va déclencher plusieurs invite auxquelles il va falloir répondre :

```
Generating a 2048 bit RSA private key
.....................................+++
.....................................+++
writing new private key to 'www.cabare.net.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) [AU]:FR
```

Country Name (2 letter code) : il s'agit du code pays (Exemple : FR)

```
State or Province Name (full name) [Some-State]:ISERE
```

State or Province Name (full name) : le département

```
Locality Name (eg, city) []:FONTAINE
```

Locality Name (eg, city) : la ville

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cabaré Michel
```

Organization Name (eg, company)

Pour les particuliers : nom et prénom

Pour les professionnels : la raison sociale telle qu'elle apparait sur Infogreffe (obligatoire)

```
Organizational Unit Name (eg, section) []:Grenoble Alpes Formation
```

Organizational Unit (eg, section) : optionnel

```
Common Name (e.g. server FQDN or YOUR name) []:www.cabare.net
```

Common Name (eg, server FQDN or YOUR name)

On indique "www.votre-domaine.fr" ce qui sécurisera également "votre-domaine.fr".

> **N.B**: Si on vous renseigne "votre-domaine.fr", l'adresse "www.votre-domaine.fr" ne sera pas sécurisée.
>
> **N.B**: Certificat SSL Wildcard : Renseignez : *.votre-domaine.fr en tant que Common Name, (a déconseiller !)

```
Email Address []:
```

Email Address : optionnel

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

optionnel

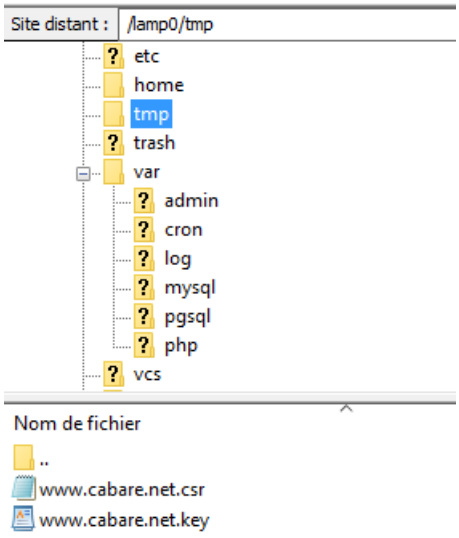
```
An optional company name []:
```

Optionnel

A la fin de la commande on obtient 2 fichiers, crées avec le nom de domaine à protéger, la **CSR** en **.csr** et la **clé privée** en **.key.** Que l'on peut voir par **ls**

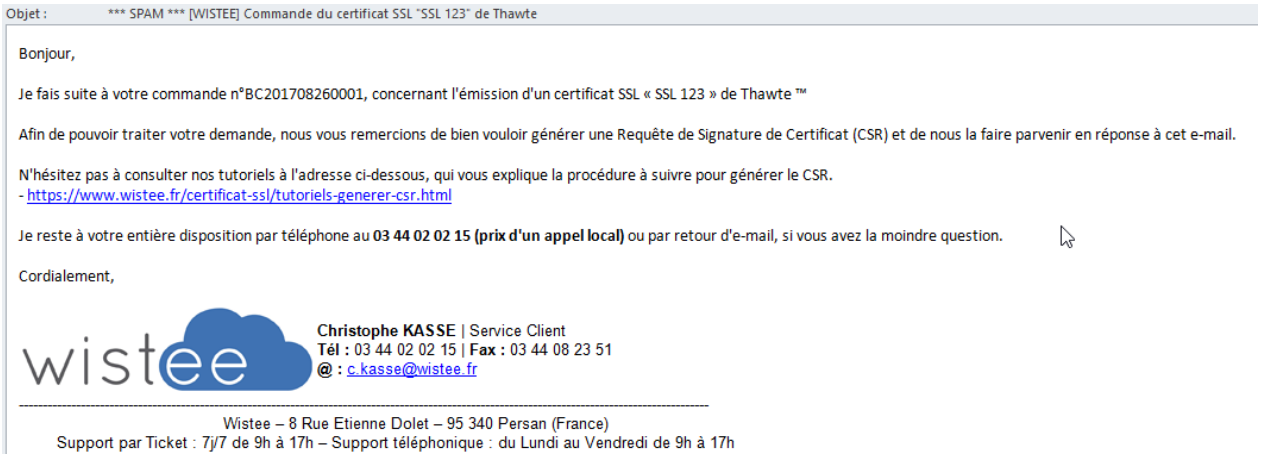
```
hosting-user@milo:/srv/data/tmp$ ls
www.cabare-formation.fr.csr  www.cabare-formation.fr.key
```

On retrouve bien sur ces 2 fichiers dans notre instance, accessibles via SFTP dans le dossier tmp



Envois Demande de certificat CSR par mail a WISTEE

Il faut envoyer la **demande de certificat CSR** par mail à WISTEE pour que la demande soit traitée…



Traitement de la Demande de certificat par WISTEE

Wistee va instancier la demande de certificat, et on doit valider l'appartenance/propriété du domaine via un mail de confirmation (exemple)

isp_enrollmentprocess@thawte.com
Envoyé : mar. 29/08/2017 09:15
À : webmaster@cabare.net

Cher,

vous avez reçu cet e-mail parce que vous êtes listé en tant que propriétaire du domaine www.cabare.net. La personne identifiée ci-dessous a fait la requête d'un Certificat SSL pour:

https://www.cabare.net

Informations du demandeur:

Nom: Christophe Kasse
E-mail: c.kasse@wistee.fr
Tel: +33 344 02 02 15

Nous vous invitons à cliquer sur l'URL ci-dessous pour revoir et approuver la demande de certificat.

https://products.thawte.com/orders/A.do?p=Ph7N446%2F3IWNkCn56%2B0ofA%3D%3D&id1=2810997

Dans lequel on doit vérifer l'exactitude des renseignements, et **approuver** Et on a un quitus d'approbation

Réception des certificats émis par WISTEE

Wistee va envoyer dans les 24-48h un mail avec en pièce jointe le certificat de la part du CA, qui peut bien sur varier(**Thawte**, **Trustprovider, geoTrustGlobalCa**…)

***** SPAM *** [WISTEE] Certificat SSL pour www.cabare.net**

Christophe KASSE - Wistee.fr <c.kasse@wistee.fr>
Envoyé : mar. 29/08/2017 09:50
À : c.kasse@wistee.fr

Message | logo-wistee.png (7 Ko) | Pièce jointe sans titre 00035.htm (2 Ko) | www.cabare.net.zip (12 Ko) | Pièce jointe sans titre 00038.htm (348 o)

Bonjour,

Veuillez trouver ci-joint votre certificat SSL "**SSL 123**" émis par Thawte ™ :

Common Name : www.cabare.net

Date d'émission : 29/08/2017
Date d'expiration : 30/08/2018

A l'intérieur de l'archive "www.cabare.net.zip" ci-jointe, vous trouverez les certificats SSL émis par l'Autorité de Certification (Thawte ™):

- **www.cabare.net.cer :** Votre certificat SSL, qui sécurise l'adresse www.cabare.net ;

- **thawteDVSSLCA-G2.cer :** Le certificat SSL intermédiaire ;
- **thawtePrimaryRootCA.cer :** Le certificat SSL racine ;

Certains serveurs / logiciels peuvent nécessiter l'importation des certificats dans un format / ordre spécifique.
Pour vous éviter de devoir convertir ou concaténer les certificats SSL ci-dessus, vous les trouverez ci-joint (dossier autres-formats).

- www.cabare.net.p7b : Certificat SSL au format PKCS #7 (.p7b). Il contient les 3 certificats SSL ci-dessus dans un seul et même fichier ;
- **racine+intermediaire.pem :** Concaténation du certificat SSL racine puis du certificat SSL intermédiaire (format x509) ;
- **intermediaire+racine.pem :** Concaténation du certificat SSL intermédiaire puis du certificat SSL racine (format x509) ;

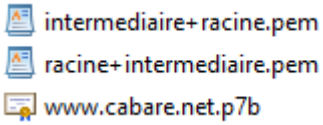
N'hésitez pas à consulter notre documentation pour obtenir toutes les informations utiles à l'installation du certificat SSL sur votre serveur :
https://www.wistee.fr/certificat-ssl.html

www.cabare.net.zip

On a dedans effectivement pas mal de choses :

Nos 3 certificats **.cer** cités

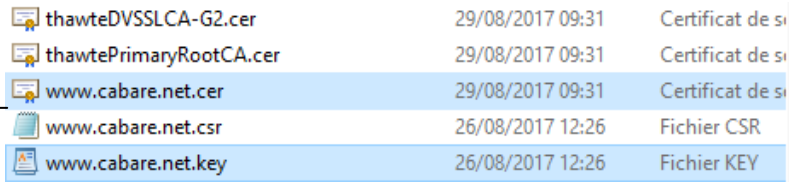
Et aussi notre certificat SSL au format **PKCS#7**



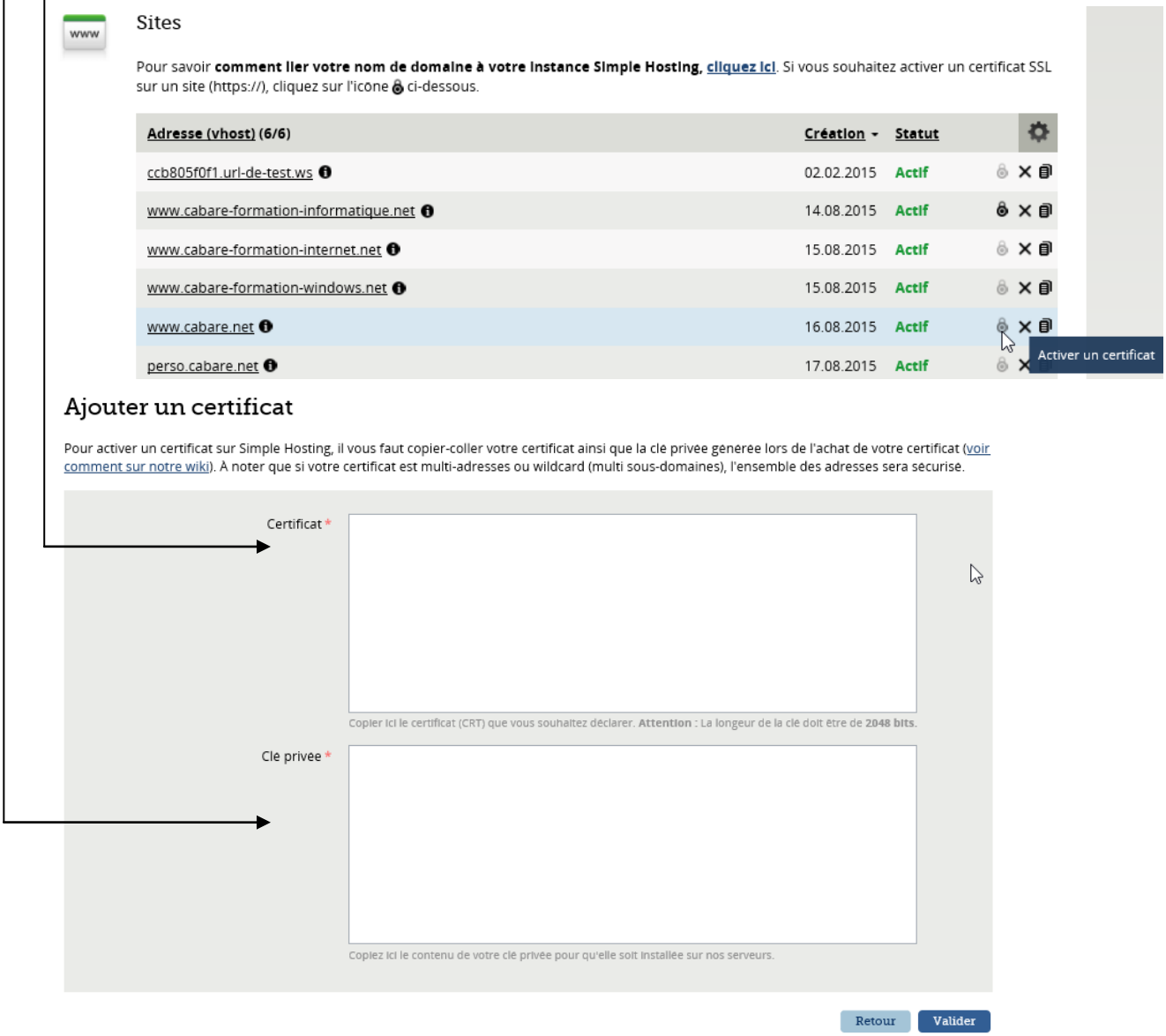
Installation du certificat sur le serveur Linux Simple Hosting

Une fois en possession au minimum

- De la clé privée
- Du certificat SSL



On peut installer le certificat sur notre instance **Simple Hosting**



ANNEXE1 : TYPE & CONVERTION DE CERTIFICATS

Types de certificats csr - cer/crt – pkcs#7 - pfx/p12:

Différents types de certificats existent, selon ce qu'ils contiennent et leur origine. On distingue essentiellement d'un côté ceux contenant la clé privée et d'un autre ceux ne la contenant pas.

- On utilisera un **.csr** pour effectuer des demandes de certificat pour un domaine précis auprès du **CA** c'est-à-dire de l'**Autorité de Certification**)
- On peut récupérer une clé au format **.key (**environnement **linux),** dans l'environnement **Windows** la clé privée reste dans le serveur depuis lequel on a effectué la **CSR.**
- On récupère les certificats demandés pour un domaine au format .**crt ou .cer**
- On pourra éventuellement convertir ces certificats **.crt ou .cer** à l'aide de la clé au format **.key** et du mot de passe associé en format **.p12** (ou **.pfx** car c'est le même format, seule l'extension change)
- A partir d'un certificat déjà installé sur un serveur (Windows), on peut extraire un certificats **.pfx ou .p12** associé à un mot de passe (car à ce moment-là il contient la clé privée)

Certificate Signing Request (.csr)

Certificat est généré par des applications pour effectuer une demande auprès des autorités de certification ! ils sont codés en base64 et contenus entre 2 phrases clés"—BEGIN NEW CERTIFICATE REQUEST—" et "—END NEW CERTIFICATE REQUEST—".

Base64-encoded ou DER-encoded binary X.509 Certificate (.cer ou .crt)

Ne contient pas de clé privées, ni de chemin. codés en base64 ou encodés et contenus entre 2 phrases clés"—BEGIN NEW CERTIFICATE REQUEST—" et "—END NEW CERTIFICATE REQUEST—"

C'est un format utilisé souvent pour "exporter " des certificats

N.B: entre **.cer** ou **.crt** seule l'extension change, le fichier est identique !

Cryptographic Message Syntax Standard (PKCS#7) Certificate (.p7b, .p7r ou .spc)

Appelé communément **PKCS#7** ne contient pas de clé privées mais peut contenir plusieurs certificats. Utilisé généralement par l'autorité de certification **CA** pour envoyer des certificats à ses clients

Personal Information Exchange Format (PKCS#12) Certificate (.pfx ou .p12)

Appelé communément **PKCS#12** contient la clé privées protégée par un mot de passe . Seul format incorporant la clé privée ! associés à un mot de passe qu'il ne faut absolument pas oublier (aucun moyen de le retrouver)

.pfx est une implémentation plutôt Windows

.p12 est une implémentation plutôt Linux

N.B: seule l'extension change, le fichier est identique !

Privacy-enhanced Electronic Mail (.pem)

Ce format est typiquement utilisé par OpenSSL pour se créer une clé privées depuis un fichier .pfx/.p12. peut contenir plusieurs certificat.

Private-key (.key)

Ce format contient la clé privées d'un certificat. Dans le monde windows il n'y a pas de mécanisme pour extraire la clé d'un certificat qui la contiendrait, ce n'est jamais nécessaire. Mais dans le monde linux-java-unix OpenSSl permet de faire ce genre de chose

ANNEXE 2 : RECUPERER 1 CERTIFICAT INSTALLE

Récupérer 1 certificat (.pfx) depuis 1 certificat installé sur 1 serveur Windows

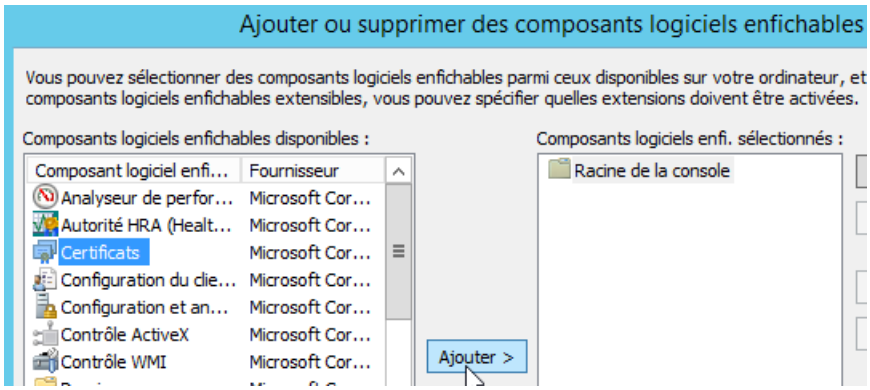
Il est possible de récupérer le certificat posé sur le serveur IIS via

- Une mmc et un assistant qui permet de gérer les certificats ordinateurs
- Une commande en ligne du type OpenSSL

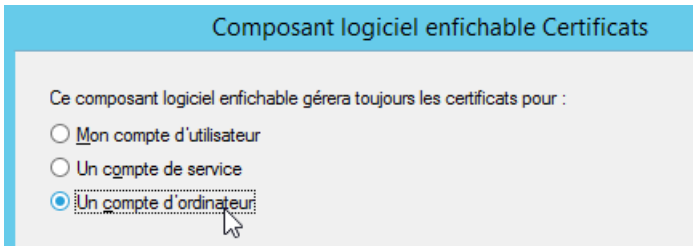
Méthode Serveur Windows vers pfx

Il faut se créer une mmc **gestion de certificats ordinateurs**

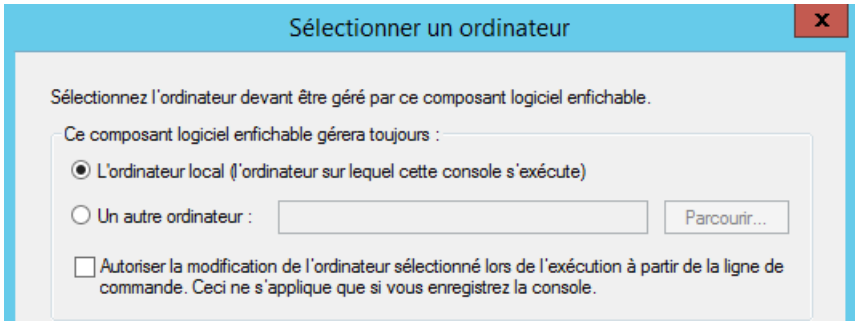
Mmc puis **ajout suppression de composant logiciels enfichable / certificats**

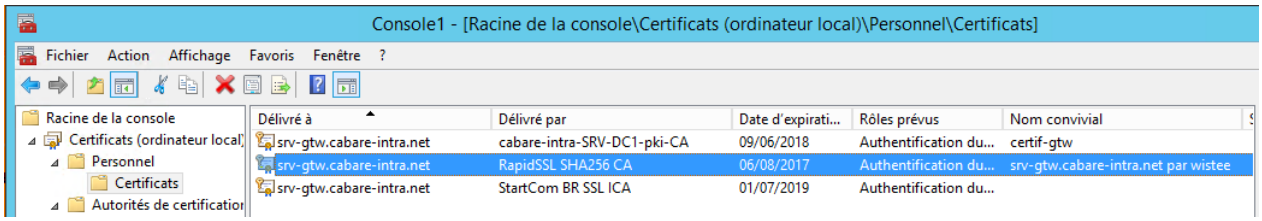


On demande **un compte d'ordinateur**

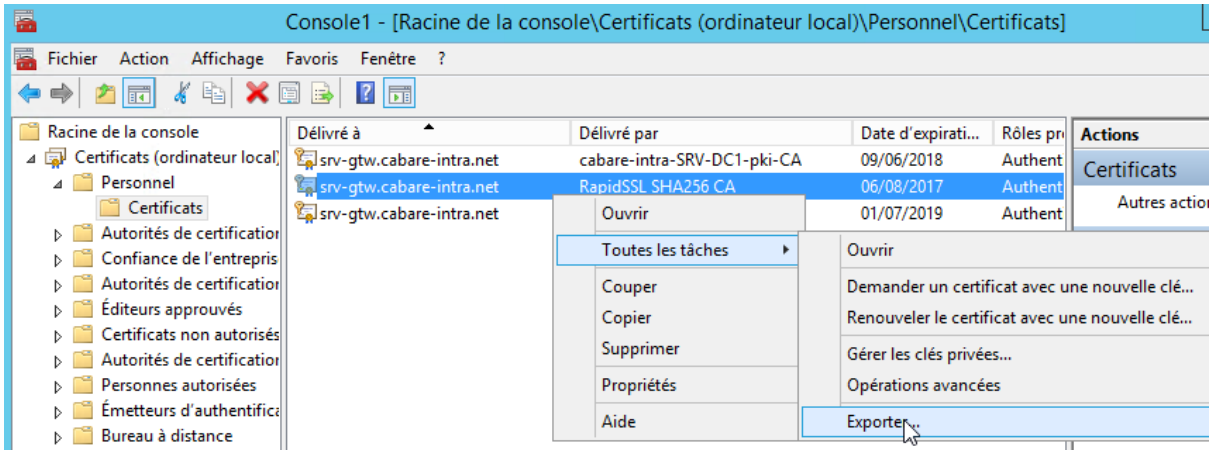


L'ordinateur local



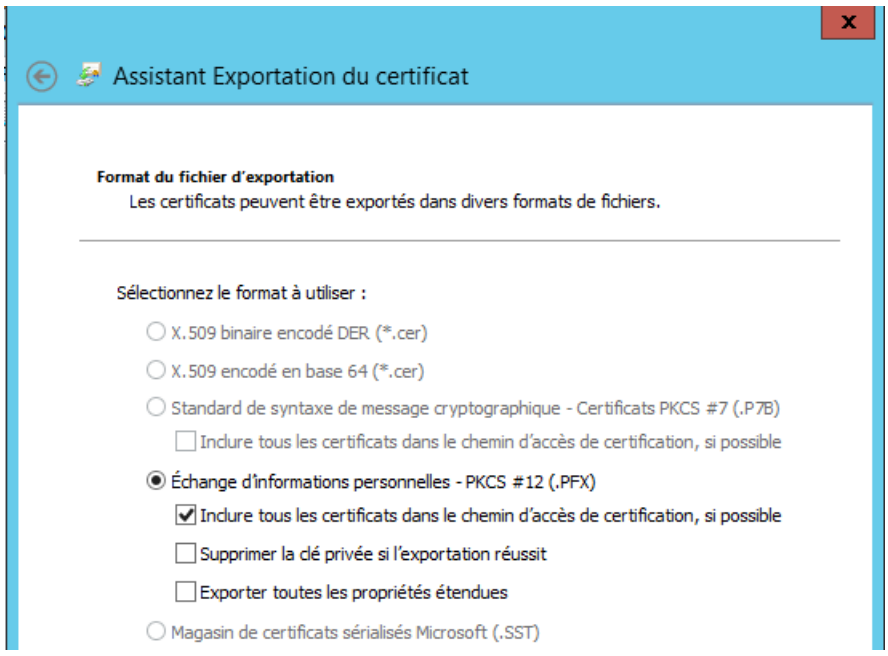


Après avoir sélectionné notre certificat, on demande via clic droit / **exporter**

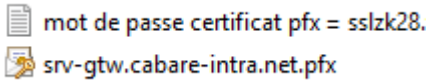


On demande d'exporter avec la clé privé (+ un mot de passe : sslzk28)

On spécifie le format voulu, dans l'exemple, .PFX



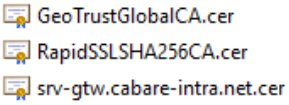
Et on obtiendra un **certificat .pfx** que l'on pourra utiliser dans la console RDS



N.B: lorsque l'on exporte un certificat incorporant la clé privée, par exemple **pfx**, il est fondamental de ne pas perdre le mot de passe donné au moment de l'export.

Méthode commande Open SSL

Un tutoriel est fourni sur wistee pour convertir un certificat au format cer vers pfx. Il faut donc partir des 3 certificats cer obtenus…



Bonjour,

.cer vers .pfx : https://www.wistee.fr/tutoriels-ssl/convertir-openssl.html

Cordialement,

ANNEXE3 : CONSOLE SSH GANDI SUR SIMPLE HOSTING

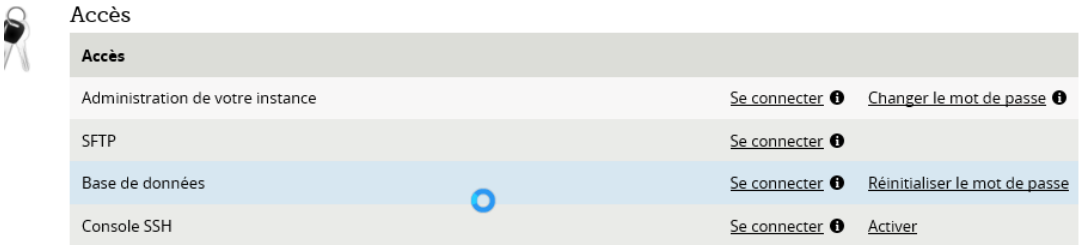
Console SSH et Putty

La console **Putty** via **SSH** c'est le moyen de passer une commande a distance directement sur le Host Gandi. 2 étapes sont requises :

- Il faut d'abord activer la connexion **SSH** sur l'instance
- Puis paramétrer la console **Putty** pour accéder à l'instance

Activation de la console SSH sur l'instance

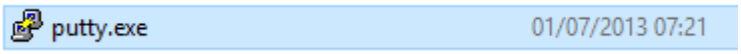
via l'interface d'administration de l'instance…



Après confirmation

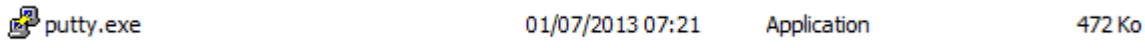
La **console SSH** se désactivera automatiquement après 2h.

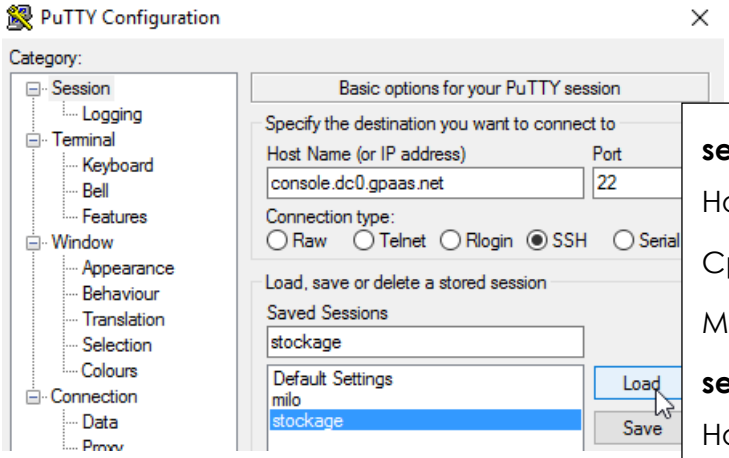
Console putty



Puis on peut lancer **putty** en utilisant les paramètres SSH

donc





serveur stockage:

Host Name : **console.dc0.gpaas.net**

Cpt : **2949292**

Mdp : **Gandistockzk28**

serveur milo

Host Name : **console.dc0.gpaas.net**

Cpt : **3802978**

Mdp : **Gandimilozk28**

serveur milo7

Host Name : **console.dc0.gpaas.net**

Cpt : **7867392**

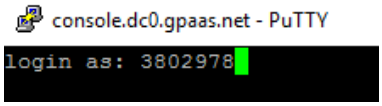
Mdp : **Gandimilo7zk28**

L'adresse de la console est toujours

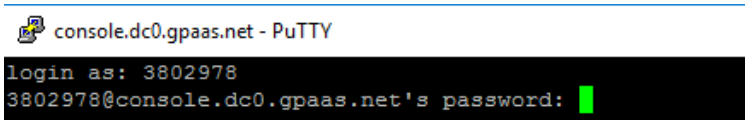
Host Name : **console.dc0.gpaas.net**

Seul les login / mdp changent :

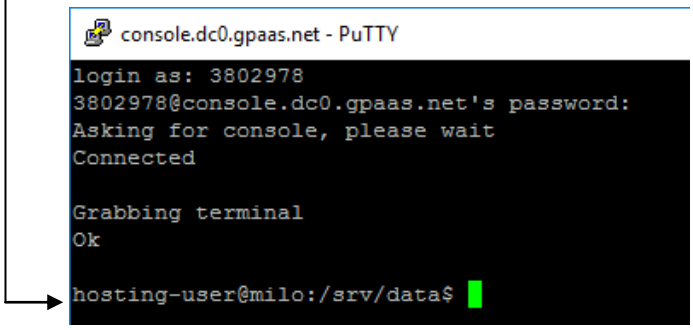
Donc selon le login (par exemple ***3802978***)



et le mot de passe (***Gandimilozk28***)



On obtient un accès sur le serveur voulu (***milo***)



Lecture de Log

Et on va chercher les fichiers de log en **/var/log** par **cd /var** suivit de **cd log**

```
hosting-user@milo:/srv/data$ cd var
hosting-user@milo:/srv/data/var$ cd log
hosting-user@milo:/srv/data/var/log$ ls
apache  boot  cron  db  www
hosting-user@milo:/srv/data/var/log$
```

Un **ls** donne les fichier/dossier, => **/var/log/apache/*** : Apache web server log files directory, et on peut lire un fichier log avec la commande **TAIL** comme

```
admin@serveur-michel:/var/log/apache2$ tail error.log
[Mon Jul 01 13:23:38 2013] [error] (12)Cannot allocate memory: fork: Unable to f
ork new process
[Mon Jul 01 17:46:53 2013] [error] (12)Cannot allocate memory: fork: Unable to f
ork new process
```

ANNEXE4 : VERIFICATION CLE PRIVEE – CERTIFICAT

Vérifier si une clé privée correspond à un certificat

Comment vérifier si une clé privée correspond bien à son certificat ?

Une clé privée contient une série de nombres. Deux de ces nombres forment la "clé publique", les autres appartiennent à la "clé privée". Les bits de la "clé publique" sont inclus quand vous générez une CSR, et font par conséquent partie du certificat associé.

Pour vérifier que la clé publique contenue dans votre certificat correspond bien à la partie publique de votre clé privée, il vous suffit de comparer ces nombres. Pour afficher le certificat et la clé, utilisez cette commande :

$ openssl x509 -noout -text -in server.crt

$ openssl rsa -noout -text -in server.key

Les parties `modulus' et `public exponent' doivent être identiques dans la clé et le certificat. Comme le `public exponent' est habituellement 65537, et comme il est difficile de vérifier visuellement que les nombreux nombres du `modulus' sont identiques, vous pouvez utiliser l'approche suivante :

$ openssl x509 -noout -modulus -in server.crt | openssl md5

$ openssl rsa -noout -modulus -in server.key | openssl md5

Il ne vous reste ainsi que deux nombres relativement courts à comparer. Il est possible, en théorie que ces deux nombres soient les mêmes, sans que les nombres du modulus soient identiques, mais les chances en sont infimes.

Si vous souhaitez vérifier à quelle clé ou certificat appartient une CSR particulière, vous pouvez effectuer le même calcul sur la CSR comme suit :

$ openssl req -noout -modulus -in server.csr | openssl md5