



<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	4
Pourquoi du SSL sur un site WEB:.....	4
Fonctionnement en http sur un site WEB:	4
Fonctionnement en https – SSL sur un site WEB:.....	4
Certificats SSL – DV – OV- EV:	5
Redirection 301 – permanente – (http sur https):	5
Certificats Wistee	7
Offre possible:.....	7
Login Wistee:.....	7
Logique procedure certificats	8
Procédure pour certificat SSL.....	8
Demande CSR de certificat	8
Depuis une machine Windows – (CSRW)	8
Depuis une machine Linux – (CSRL)	8
Récupération du Certificat SSL émis par le CA	9
Via Wistee	9
Via Gandi	9
Installation du Certificat SSL reçu (et activation application SSL)	9
Sur une machine Windows.....	9
Sur une machine Gandi instance Simple Hosting - Linux	9
Certificat WISTEE sur serveur Windows	10
Demande de certificat CSR – via Windows CSRW	10
Envois Demande de certificat CSR par mail a WISTEE	11
Traitement de la Demande de certificat par WISTEE	12
Réception des certificats émis par WISTEE	13
Installation du certificat PKCS#7 Sur le Serveur Windows	14
Terminer la demande depuis Windows Internet Server.....	15
insérer un certificat dans RDS	17
A partir de certificat pfx (ou p12):	17
Certificat GANDI sur instance Simple Hosting	19
Demande de certificat CSR – via Linux Gandi (console SSH) CSRL	19
Lancement console SSH.....	19
Placement en Invite de Comande	19
Commande OPENSSL	20
Envois Demande de certificat CSR via site web Gandi.....	21
Traitement Demande de certificat par Gandi.....	25
Réception des certificats émis par Gandi	26
Installation du certificat sur le serveur Linux Simple Hosting	28
Certificat intermédiaire, ou non.....	29
Forcer https sur Simple Hosting avec .htaccess (base)	30
Redirection http + https de domaine sur www.domaine (complet)	30
Logo validation https sur Simple Hosting avec certificat standard.....	31
Certificat WISTEE sur instance Gandi Simple Hosting	32
Demande de certificat CSR – via Linux Gandi (console SSH) CSRL	32
Lancement console SSH.....	32
Placement en Invite de Comande	32
Commande OPENSSL	33

Envois Demande de certificat CSR par mail a WISTEE	34
Traitement de la Demande de certificat par WISTEE	35
Réception des certificats émis par WISTEE	35
Installation du certificat sur le serveur Linux Simple Hosting	36
Annexe1 : type & conversion de certificats.....	37
Types de certificats csr - cer/crt – pkcs#7 - pfx/p12:.....	37
Annexe 2 : Recuperer 1 certificat installé	39
Récupérer 1 certificat (.pfx) depuis 1 certificat installé sur 1 serveur Windows.....	39
Méthode Serveur Windows vers pfx	39
Méthode commande Open SSL	41
Annexe3 : console SSH gandi sur simple hosting	42
Console SSH et Putty	42
Activation de la console SSH sur l'instance	42
Console putty.....	42
Lecture de Log	43
Annexe4 : Vérification clé privée – certificat	44
Vérifier si une clé privée correspond à un certificat	44

SSL ET SITE WEB

Pourquoi du SSL sur un site WEB:

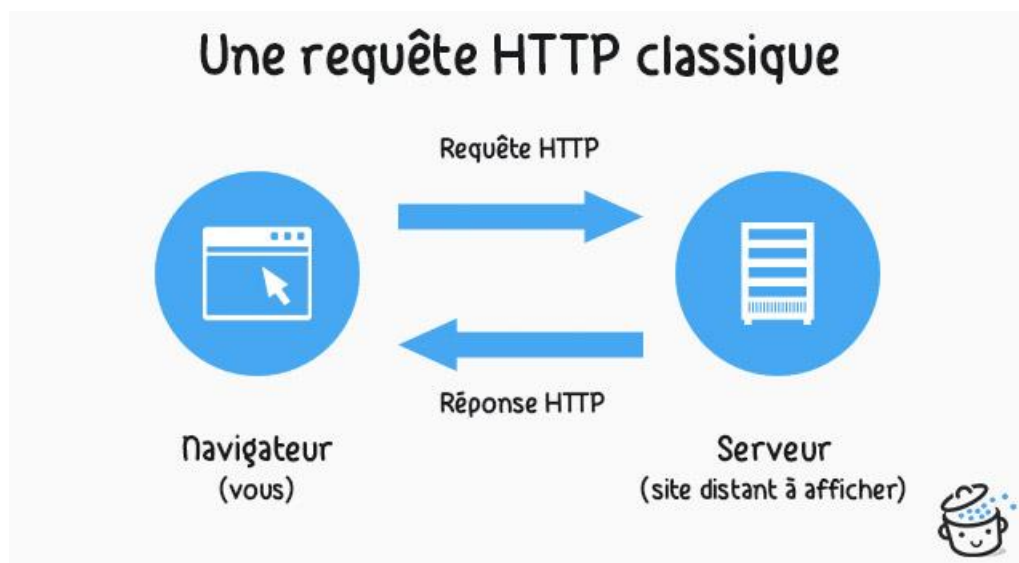
Depuis août 2014, Google communique sur l'importance des sites en **HTTPS** (c'est-à-dire avec la présence d'un **certificat SSL**). Avoir un site en **HTTPS** est devenu un critère de pertinence dans l'algorithme de Google : les sites sécurisés ont pu constater un meilleur positionnement dans les résultats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



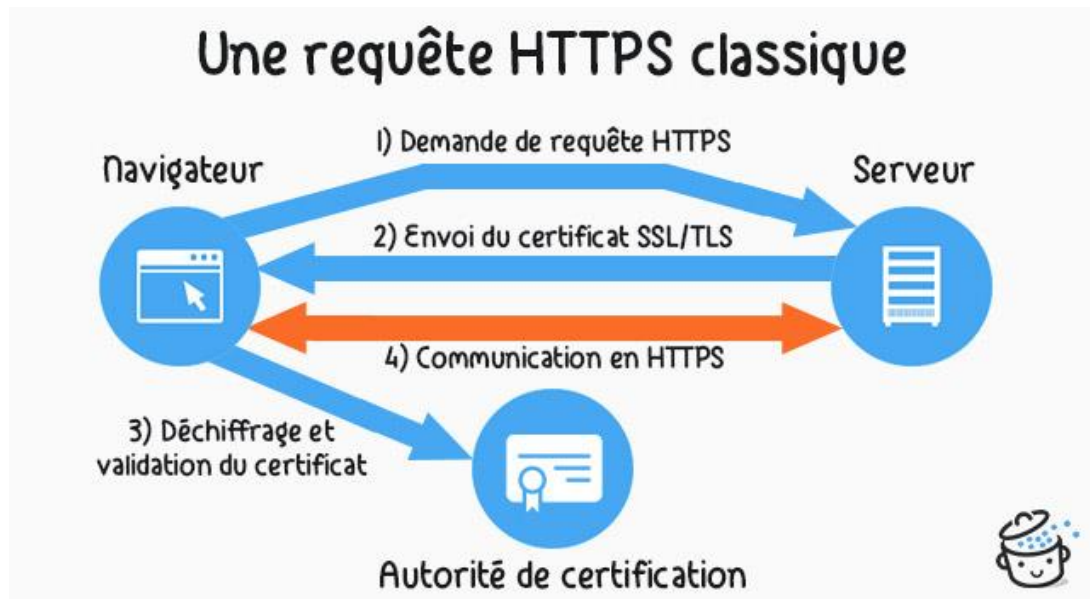
Fonctionnement en https – SSL sur un site WEB:

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 jusqu'à ce 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 détentricice 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 transmettez 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 intéresse 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

 .htaccess - Bloc-notes

Fichier Edition Format Affichage ?

```
RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

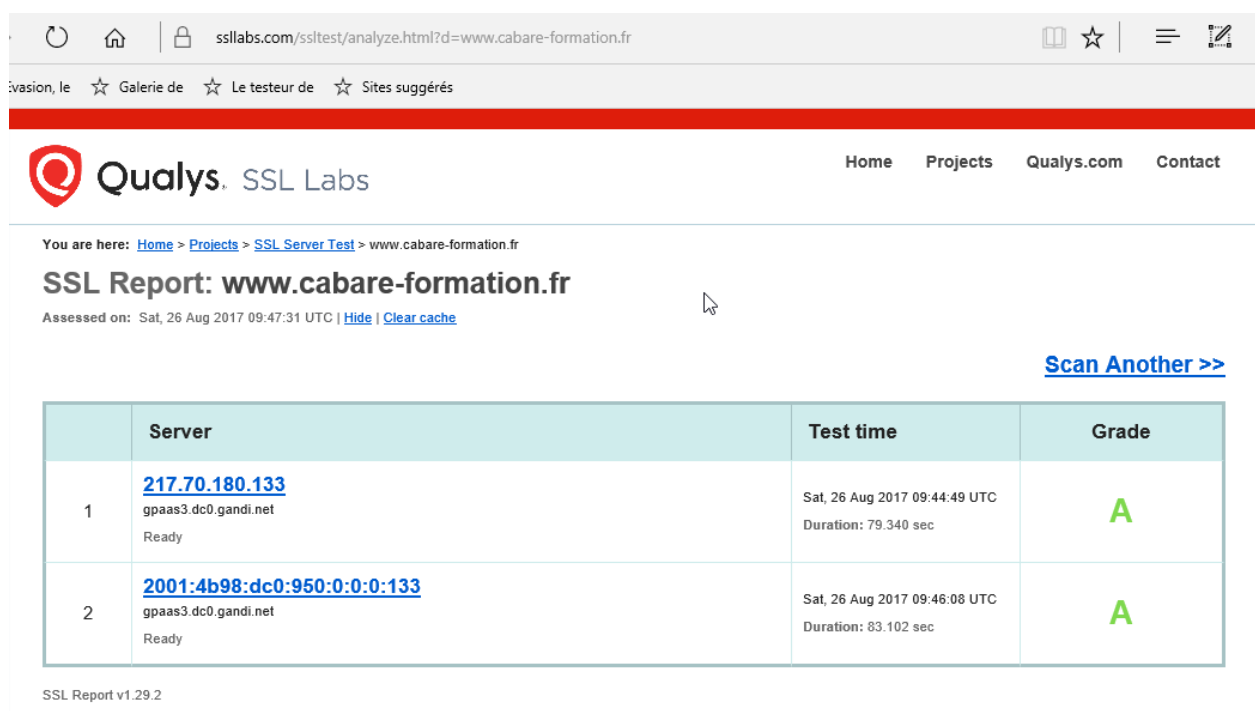
N.B: Si le port utilisé n'est pas le port 80 (?) alors on peut écrire la condition suivante

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



The screenshot shows a web browser displaying the Qualys SSL Labs report for the website www.cabare-formation.fr. The browser's address bar shows the URL ssllabs.com/sslttest/analyze.html?d=www.cabare-formation.fr. The report header includes the Qualys SSL Labs logo and navigation links: Home, Projects, Qualys.com, and Contact. Below the header, the report title is "SSL Report: www.cabare-formation.fr", and it notes the assessment date as "Sat, 26 Aug 2017 09:47:31 UTC". A "Scan Another >>" link is visible on the right. The main content is a table with two columns: "Server" and "Test time", and a "Grade" column. The table shows two test results, both with a grade of "A".

	Server	Test time	Grade
1	217.70.180.133 gpaas3.dc0.gandi.net Ready	Sat, 26 Aug 2017 09:44:49 UTC Duration: 79.340 sec	A
2	2001:4b98:dc0:950:0:0:0:133 gpaas3.dc0.gandi.net Ready	Sat, 26 Aug 2017 09:46:08 UTC Duration: 83.102 sec	A

SSL Report v1.29.2

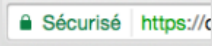
CERTIFICATS WISTEE

Offre possible:

Bien de choses interviennent, notamment multi domaine, multi-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 sécurité **EV Extended Validation** est à 200 Euro...

	wistee SSL DV	thawte™ SSL 123
CARACTÉRISTIQUES DU CERTIFICAT SSL		
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		
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	✗	

Login Wistee:

Login **CMC3-WISTEE**

Mdp **wisteeJb62**

■ Accès à votre compte client



Identifiant :

Mot de passe :

LOGIQUE PROCEDURE CERTIFICATS

Procédure pour certificat SSL

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

- D'abord 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 à 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'Autorité de certification, mais plutôt simplement par le fournisseur du certificat. Evidemment les procédures 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 reçu 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

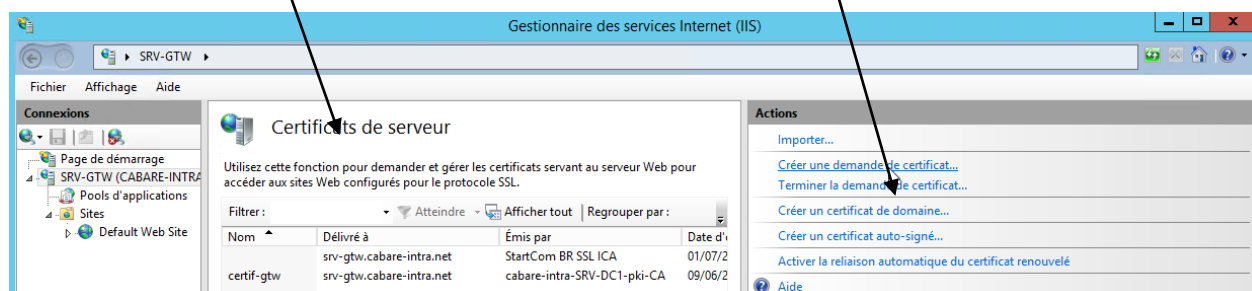
On peut faire la demande CSR depuis le serveur IIS sur lequel on souhaite installer le certificat

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**



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

Demande de certificat

Propriétés du nom unique

Indiquez les informations requises pour le certificat. Lorsque vous entrez le département ou région et la ville/localité, utilisez des noms complets et officiels, et n'employez aucune abréviation.

Nom commun :

Organisation :

Unité d'organisation :

Ville :

Département/région :

Pays/région :

Précédent Suivant Terminer Annuler

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

?

x



Propriétés du fournisseur de services de chiffement

Sélectionnez un fournisseur de services de chiffement et une longueur en bits. La longueur en bits de la clé de chiffement détermine l'efficacité du chiffement du certificat. Avec une clé de chiffement plus longue, la sécurité est accrue. Toutefois une longueur trop importante peut nuire aux performances.

Fournisseur de services de chiffement :

Microsoft RSA Schannel Cryptographic Provider

Longueur en bits :

2048

Et ensuite on pose le CSR où l'on veut

?

x



Nom du fichier

Indiquez un nom de fichier pour la demande de certificat. Ces informations peuvent être envoyées à une autorité de certification en vue de la signature.

Indiquer un nom de fichier pour la demande de certificat :

...

Pour obtenir la clé publique .cer



Ce fichier contient la demande de certificat, clé publique codée

```
demande-csr-srv-gtw-wistee.txt
```

Fichier Edition Format Affichage ?

```
|-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIEkjCCA3oCAQAwgZAx CzA JBgNVBAYTAkZSMQ8wDQYDVQQIDAZpc80ocmUxETAP  
BgNVBAcMCEZvb nRhaW5IMRcwFQYDVQQKDA5DYWJhc sOpIE1pY2h1bDEhMB8GA1UE  
CwwYR3J1bm9ibGUGQXwxZXMG Rm9ybWF0aW9uMESEewHwYDVQQDDhcnYtTzR3LmNh  
YmFyZS1pb nRyYS5uZXQwg gEiMA0GC SGqSI b3DQEBAQUAA4IBDwAwggEKA oIBA QDZ  
09dsrTj z7FL4id55gkNaKVlE7KJ6jvz +E2Fm95DrWUrL9XPUIH/FmTVXR4d8eJd5  
TUDCGX-Fl273-jcYm-M10h-G-S3-Y5Zh-N-XB373-LQYw-F-1-t-/YnTPBhuic hlt
```

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 \[mailto:c.kasse@wistee.fr\]](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°BC2017050030, 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=AGmeV38XLU0zoxTlne74pA2sv>

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

← → ↻ 🏠 | GeoTrust, Inc. [US] products.geotrust.com/orders/A.do?p=AGmeV38XLU0zoxTlne74pA2sv

☆ Aiskep Evasion, le ☆ Galerie de ☆ Le testeur de ☆ Sites suggérés

RapidSSL.com
SSL Certificate Solutions from the World's fastest growing SSL Provider.

FreeSSL™

Révision et approbation de la commande de FreeSSL

Approbation de la commande
Veuillez examiner les informations ci-dessous pour approuver ou refuser cette demande de certificat. Pour toute question concernant la demande de certificat, veuillez contacter l'une des personnes figurant dans la liste ci-dessous ou bien l'[assistance RapidSSL.com](#).

Informations sur les commandes
ID de commande 15472628
Validité (mois) 1
Nombre de serveurs 1
Serveur Web
Instructions spÃ©ciales aucune

Informations relatives au certificat
Noms de serveurs supplÃ©mentaires srv-gtw.cabare-intra.net
Nom courant srv-gtw.cabare-intra.net
Organisation :
UnitÃ© org. Grenoble Alpes Formation
UnitÃ© org.
ID utilisateur
Pays : FR

Contacts

RÃ´le	Nom	NumÃ©ro de tÃ©lÃ©phone	Adresse Ã©lectronique	Fonction
Technique:	Christophe Kasse	+33 344 02 02 15	c.kasse@wistee.fr	Dhr
Administratif:	Christophe Kasse	+33 344 02 02 15	c.kasse@wistee.fr	Dhr
Approbateur du domaine:			webmaster@cabare-intra.net	

SÃ©lectionnez une des options ci-dessous. Si vous approuvez cette demande, le certificat sera immÃ©diatement gÃ©nÃ©rÃ©, la carte de crÃ©dit sera dÃ©bitÃ©e (si applicable) et le certificat sera envoyÃ© aux destinataires par courrier Ã©lectronique. Appuyez une seule fois sur le bouton ci-dessous ; le processus peut durer quelques secondes.

DÃ©claration de confidentialitÃ© ©2017 GeoTrust, Inc. Tous droits rÃ©servÃ©s.

On a un quitus d'approbation

☆ Aiskep Evasion, le ☆ Galerie de ☆ Le testeur de ☆ Sites suggérés

RapidSSL.com
SSL Certificate Solutions from the World's fastest growing SSL Provider.

FreeSSL™

Révision et approbation de la commande de FreeSSL

Commande approuvée
ID de la commande : 15472628

Votre commande a été approuvée et le certificat vous sera envoyé soit par courrier électronique, soit par l'intermédiaire du fournisseur de certificat. Si vous avez des questions ou si vous ne recevez pas votre certificat rapidement, contactez votre fournisseur ou l'[assistance RapidSSL.com](#).

DÃ©claration de confidentialitÃ© ©2017 GeoTrust, Inc. Tous droits rÃ©servÃ©s.

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...**)

[WISTEE] Certificat SSL pour srv-gtw.cabare-intra.net

Christophe KASSE - Wistee.fr <c.kasse@wistee.fr>

Envoyé : jeu. 06/07/2017 10:28

À : c.kasse@wistee.fr

Message logo-wistee.png (7 Ko) Pièce jointe sans titre 00075.htm (2 Ko) srv-gtw.cabare-intra.net.zip (11 Ko)
Pièce jointe sans titre 00078.htm (348 o)

Bonjour,

Veuillez trouver ci-joint votre certificat SSL "Certificat SSL : 30 Jours d'essai" émis par RapidSSL ® :

Common Name : srv-gtw.cabare-intra.net

Date d'émission : 06/07/2017

Date d'expiration : 06/08/2017

A l'intérieur de l'archive "srv-gtw.cabare-intra.net.zip" ci-jointe, vous trouverez les certificats SSL émis par l'Autorité de Certification (RapidSSL ®) :

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

- **RapidSSLSHA256CA.cer** : Le certificat SSL intermédiaire ;

- **GeoTrustGlobalCA.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).

- **srv-gtw.cabare-intra.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>

demande-csr-srv-gtw-wistee.txt	05/07/2017 19:51
srv-gtw.cabare-intra.net.zip	06/07/2017 11:49

On a dedans effectivement pas mal de choses :

GeoTrustGlobalCA.cer	06/07/2017 10:27
RapidSSLSHA256CA.cer	06/07/2017 10:27
srv-gtw.cabare-intra.net.cer	06/07/2017 10:27

Nos 3 certificats .cer cités

intermediaire+racine.pem
racine+intermediaire.pem
srv-gtw.cabare-intra.net.p7b

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.

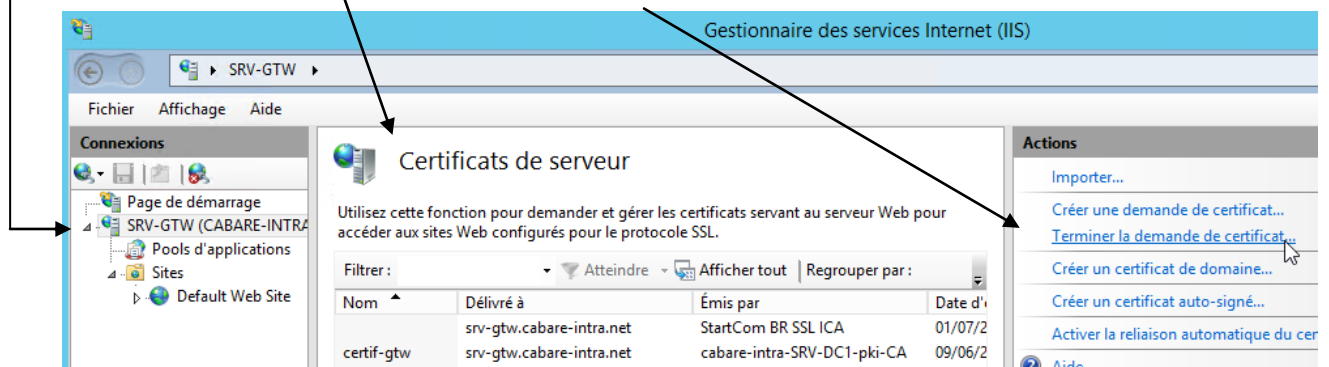
N.B: Si la requête **CSR** a été générée sur un autre serveur (Windows ou Linux), il faut importer le certificat au format **PKCS #12 (.pfx)** dans IIS

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

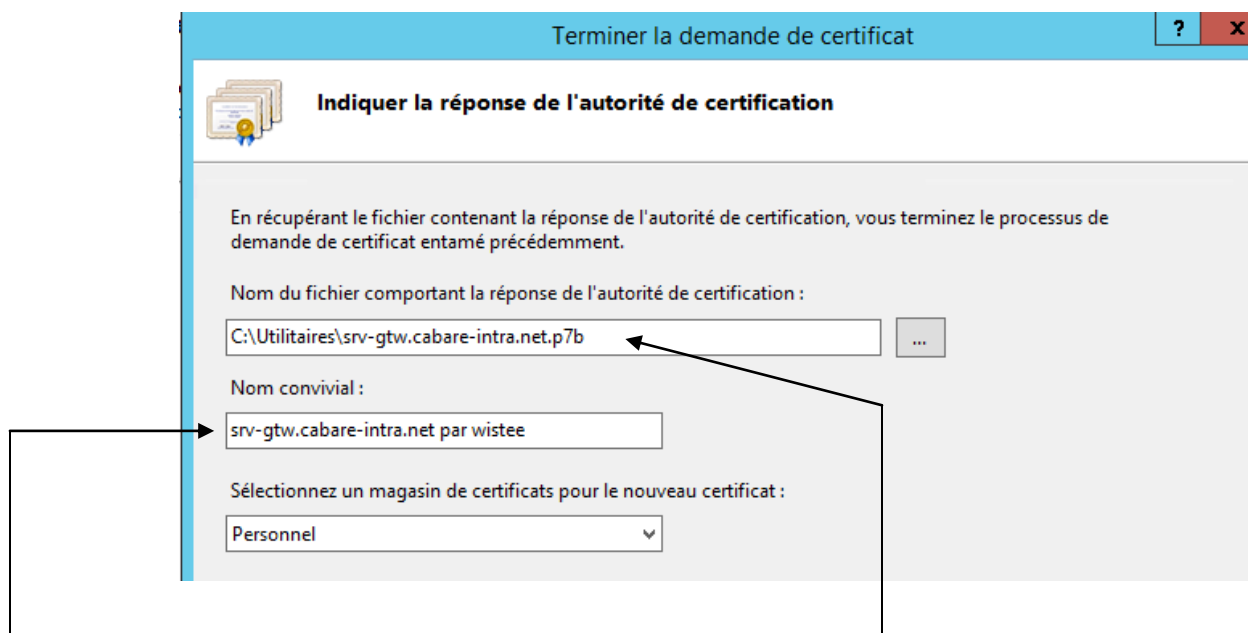
Chez **Wistee**, en plus du certificat au format **x509**, est envoyé aussi le certificat **SSL** déjà converti au format **PKCS #7 (.p7b)**.

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**



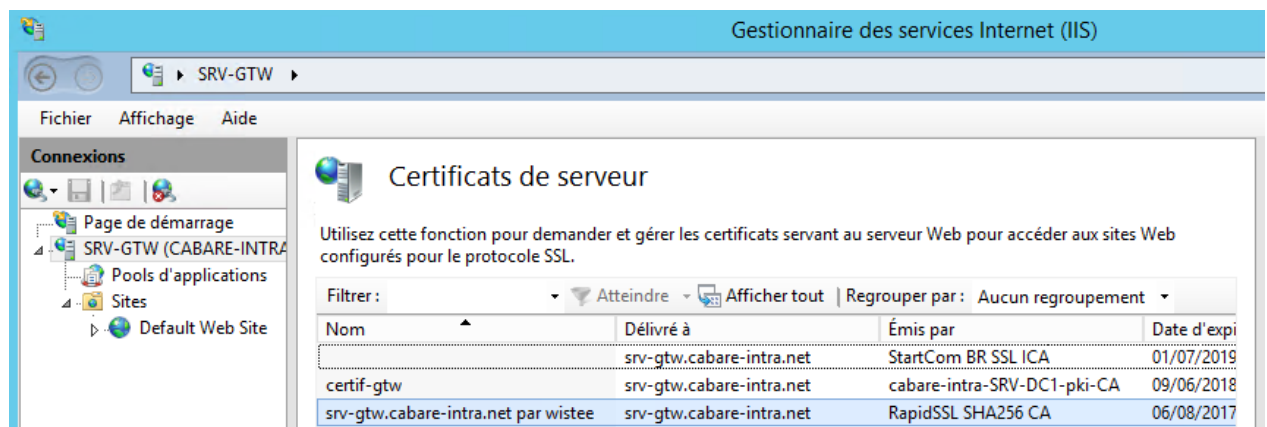
On obtient



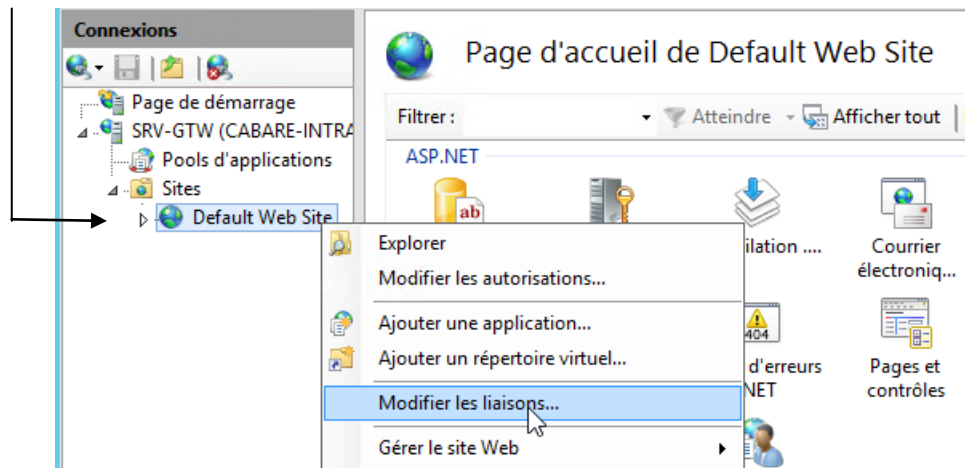
Par défaut, seuls les fichiers **".cer"** sont listés, il faut sélectionner donc ***.*** pour sélectionner le certificat SSL au format "P7B / PKCS#7".

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

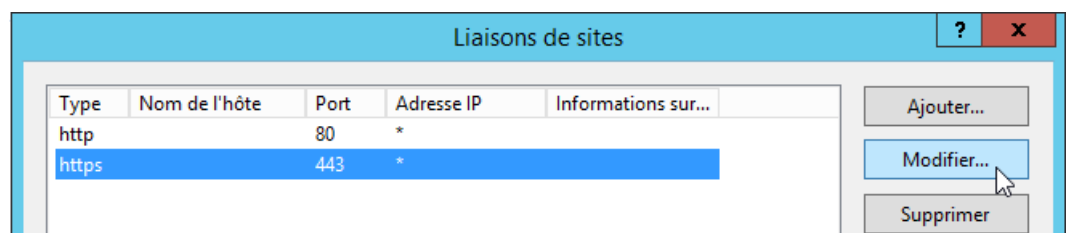
et on devrait obtenir



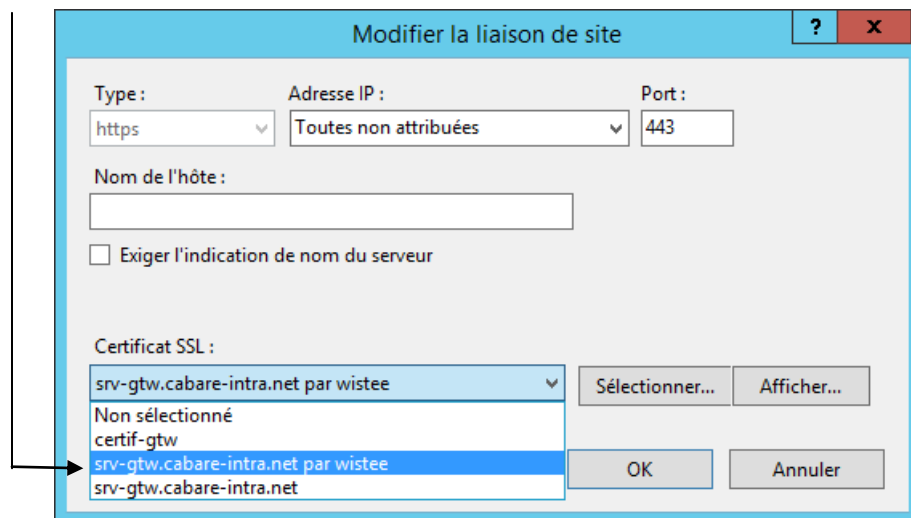
Il faut assigner le certificat à la liaison https:443, via le **site web par défaut**, puis clic droit **Modifier les liaisons**



On choisit 443 et on demande **Modifier**



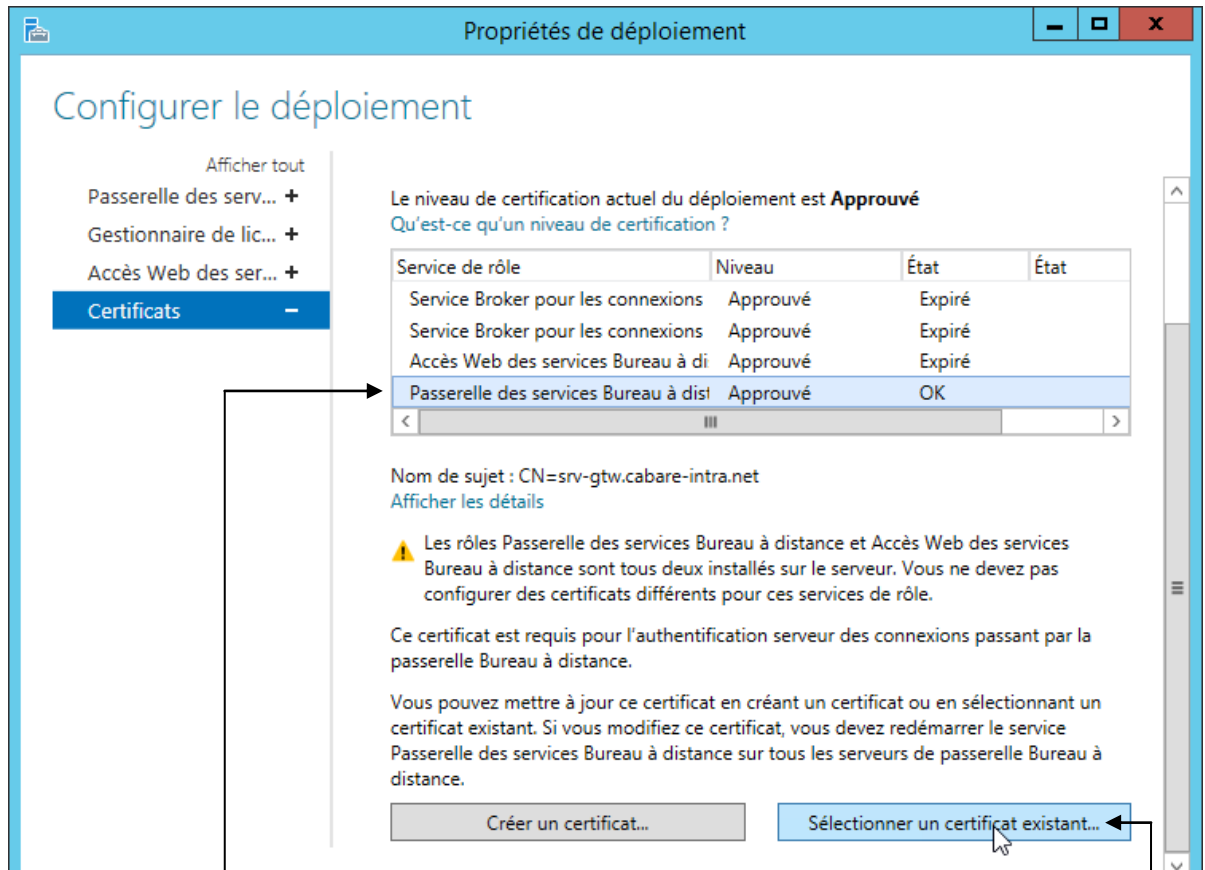
Et on choisit notre certificat avec son nom "parlant"



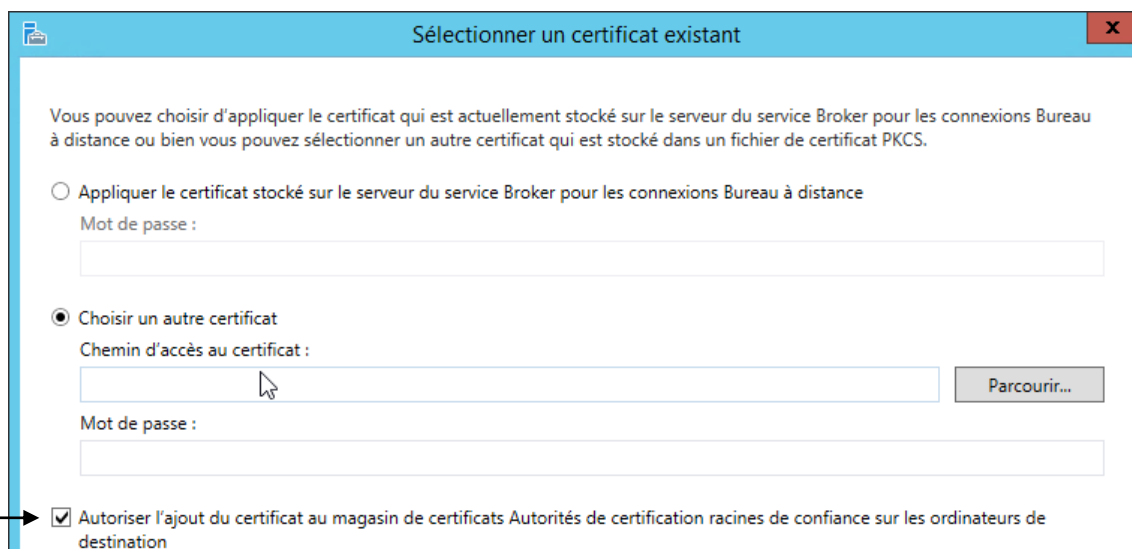
INSERER UN CERTIFICAT DANS RDS

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)

CERTIFICAT GANDI SUR INSTANCE SIMPLE HOSTING

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

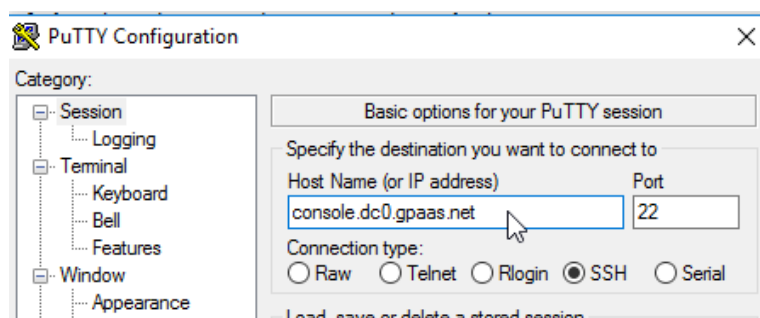
On peut faire la demande **CSR** depuis le serveur **Gandi Simple Hosting** sur lequel on souhaite installer le certificat à travers une **console SSH** (permettant ensuite de passer la commande OpenSSL, mais aussi toutes les commandes souhaitées d'ailleurs)

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.

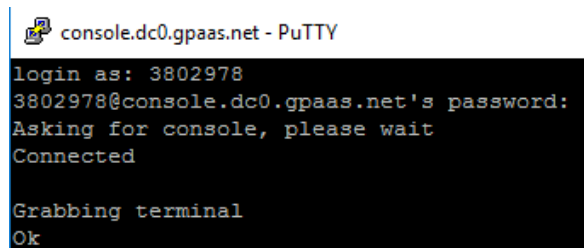
Lancement console SSH

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

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



et pour miло 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**

```
hosting-user@miло:/srv/data$ dir
db etc home tmp trash var vcs web
hosting-user@miло:/srv/data$ cd tmp
hosting-user@miло:/srv/data/tmp$ ls
hosting-user@miло:/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 -keyout 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 Formation
```

Organization Name (eg, company)

Pour les particuliers : nom et prénom

Pour les professionnels : la raison sociale telle qu'elle apparaît 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, créés 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

Site distant : /lamp0/tmp

Nom de fichier	Taille de fichier	Type de fic...
..		
www.cabare-formation.fr.csr	1 021	Fichier CSR
www.cabare-formation.fr.key	1 708	Fichier KEY

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**

gandi.net mon compte

Services | Gestion du compte | Facturation | Commandes en cours | Messages (43)

Domaines | **SSL** | Sites web | Simple Hosting | Serveurs

SSL | 6 Certificats (0) | Operations (0) | Acheter un certificat SSL

Filtrer ? [] OK [] Recherche avancée [] Exporter

Adresse sécurisée (0/0) -	Type	Expiration	Statut
---------------------------	------	------------	--------

Le **certificat SSL standard** suffirait

Certificat SSL Standard 1 adresse

1 an - 12,00 €

Choisir

Et l'on obtient

Achat d'un certificat SSL

Vous avez sélectionné un **Certificat Standard 1 domaine (1 an)**. ([changer ?](#))

Insertion de la CSR

Cette étape est primordiale, **car c'est votre CSR qui va déterminer quel nom de domaine est pris en charge par votre certificat (le CN principal dans le cas d'un multi-domaines). Si vous ne savez pas comment générer votre CSR, nous vous invitons à visiter nos pages wiki** à ce sujet. Lorsque vous insérez la CSR, une vérification automatique se lance (cliquez juste en dehors du cadre) et affiche le CN principal dans le champ sous la CSR. Ceci vous permet de vérifier que vous n'avez pas fait d'erreur de saisie. Une validation finale sera également présentée dans l'étape suivante, avec toutes les occurrences prises en compte.

CSR *

Utilisez notre [générateur](#) ou consultez notre [documentation en ligne](#) si vous souhaitez avoir plus d'informations sur ce processus.

Domaine (CN) principal

en attente de la CSR...

Ceci est le domaine principal déclaré dans votre CSR dans le champ CN. S'il n'est pas correct, vous devez refaire votre CSR.

Logiciel utilisé

Apache/ModSSL

Veuillez indiquer le logiciel qui utilisera votre certificat. ([qu'est-ce que c'est ?](#))

Retour

Valider

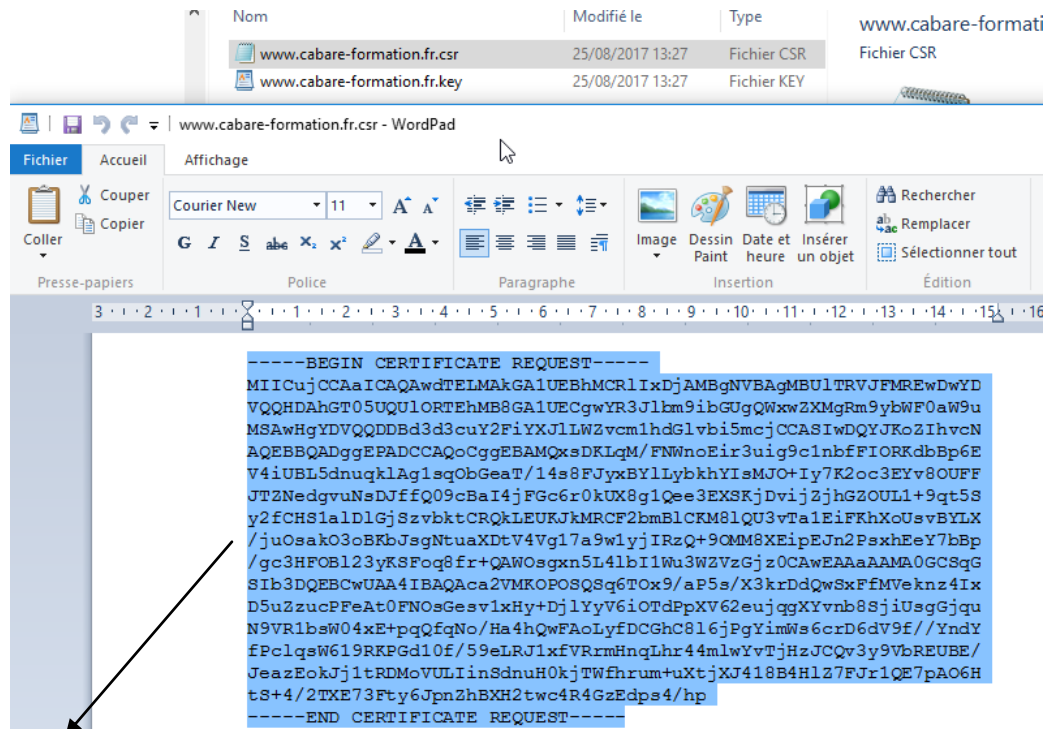
Panier

Certificat SSL		
Certificat ... ne (1 an)	12,00 €	✕
Total HT	12,00 €	
Total TTC	14,40 €	
Abandonner cette commande		

Dans cette fenêtre il va falloir alors :

- Copier coller la demande CSR obtenu via la commande OPENSSL effectuée précédemment
- 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 par la commande OPENSSL...



On le colle ici

Achat d'un certificat SSL

Vous avez sélectionné un **Certificat Standard 1 domaine (1 an)**. ([changer ?](#))

Insertion de la CSR

Cette étape est primordiale, car c'est votre CSR qui va déterminer quel nom de domaine est pris en charge par votre certificat (le CN principal dans le cas d'un multi-domaines). Si vous ne savez pas comment générer votre CSR, nous vous invitons à visiter [nos pages wiki](#) à ce sujet. Lorsque vous insérez la CSR, une vérification automatique se lance (cliquez juste en dehors du cadre) et affiche le CN principal dans le champ sous la CSR. Ceci vous permet de vérifier que vous n'avez pas fait d'erreur de saisie. Une validation finale sera également présentée dans l'étape suivante, avec toutes les occurrences prises en compte.

CSR *

```
-----BEGIN CERTIFICATE REQUEST-----
MIICujCCAaICAQAwTELMAG1UEBhMCRLIxDjAMBGNVBAgMBU1TRVJFMREwDwYD
VQHQDAhGT05UQU1ORTEhMB8GA1UECgwyR3Jlbn9ibGUGQWxwZXNMcG9yYyB0aW9u
MSAwHgYDVQDDbD3d3cuY2FiYXJlLWZvcmlhdG1vbi5mcjCCAS1wDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMQxsDKLqM/FNwNoEir3uig9c1nbFFIORKdbBp6E
V4iUBL5dnuqkAg1sqObGeaT/14s8FjyxBYlLybkhYIsmJQ+Iy7K2oc3EYv8OUFF
JTZNedgvuNsDjffQ09cBaI4jFGc6r0kUX8g1Qee3EXSKjDviJzjhGZOU1+9qt5S
y2fCHS1a1d1GjSzbvktCRQkLEUKJkMRCF2bmBlCKM81QU3vTa1EiFkhXoUsvBYLX
/juOsakO3oBKbJsgNtuaXdtV4Vg17a9wlyjIRzQ+9OMM8XEipEjn2PaxhEeY7bBp
/gc3HFOB123yKSFog8fr+QAWOsgxn5L41b1Wu3WZVzGjz0CAwEAaAAMA0GC8qG
S1b3DQEBcUAA4IBAQAca2VMKOP0S0q6TOx9/ap5s/X3krDdQwSxPfMveknz4Ix
D5uZzucPFaAt0FN0sGesv1xHy+Dj1YyV6iOTdPpXV62eujqgXYvnb8SjiUsgGjqu
N9VR1bsW04xE+pqQfQNo/Ha4hQwFAoLyfDCGhC816jPgYimW6crD6dV9f/YndY
fPclqsW619RKPgd10f/59eLRJ1xfVRrmHnqLhr44mlwYvTjHzJCQv3y9VbREUBE/
JeaZEokJj1tRDMoVULiInSdnuH0kjTWfhrum+uXtjXJ418B4H1Z7Fjr1QE7pAO6H
tS+4/2TXE73Fty6JpnZhBXH2twc4R4GzEdps4/hp
-----END CERTIFICATE REQUEST-----
```

Utilisez notre [générateur](#) ou consultez notre [documentation en ligne](#) si vous souhaitez avoir plus d'informations sur ce processus.

Domaine (CN) principal

www.cabare-formation.fr

Ceci est le domaine principal déclaré dans votre CSR dans le champ CN. S'il n'est pas correct, vous devez refaire votre CSR.

Logiciel utilisé

Apache/ModSSL

Veillez indiquer le logiciel qui utilisera votre certificat. ([qu'est-ce que c'est ?](#))

Retour

Valider

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

On annonce le tarif à 0 car on dispose de 1 certificat gratuit par domaine la 1^{re} année.

Validez votre commande

Veuillez vérifier que les éléments suivants sont corrects et valider nos contrats avant de passer à la page de paiement.

Commande

Certificat SSL

- Certificat Standard 1 domaine (1 an)

Code promotion

Si vous bénéficiez d'un [code promotion](#) ou d'un coupon, veuillez le renseigner ci-dessous et cliquer sur le bouton "Valider le code".
Attention, dans le cas d'un coupon à usage unique, une fois celui-ci valide, il ne pourra plus être réutilisé lors d'une autre commande.

Valider le code

Liste des contrats à accepter

Veuillez **lire et accepter** les contrats suivants avant de cliquer sur "Valider" :

- ☒ Conditions particulières de vente des certificats SSL ([Lire](#))

[Valider l'ensemble des contrats](#)

Retour

Valider

Panier

Certificat SSL

Certificat ... ne (1 an)	0,00 €
--------------------------	--------

Total HT	0,00 €
----------	--------

Total TTC	0,00 €
-----------	--------

[Abandonner cette commande](#)

Votre grille de prix

Le montant de vos achats sur Gandi sur les 12 derniers mois atteint **310,70 €**.
(Attention, cela ne prend pas en compte la commande en cours)

Vous bénéficiez des tarifs de la [grille de prix dégressive A](#)

Aide

- Avant de finaliser votre commande, veuillez vérifier que ces données sont exactes.
- Veuillez lire et valider nos conditions générales de vente avant de passer à l'étape suivante.
- N'hésitez pas à contacter notre service client pour plus d'informations.

Et la commande de certificat est passée!

Commande validée

Votre commande étant gratuite, elle a été automatiquement validée.

Que va-t-il se passer maintenant ?

D'ici quelques secondes, nous allons lancer votre commande, vous recevrez un email de confirmation.

Certificat SSL

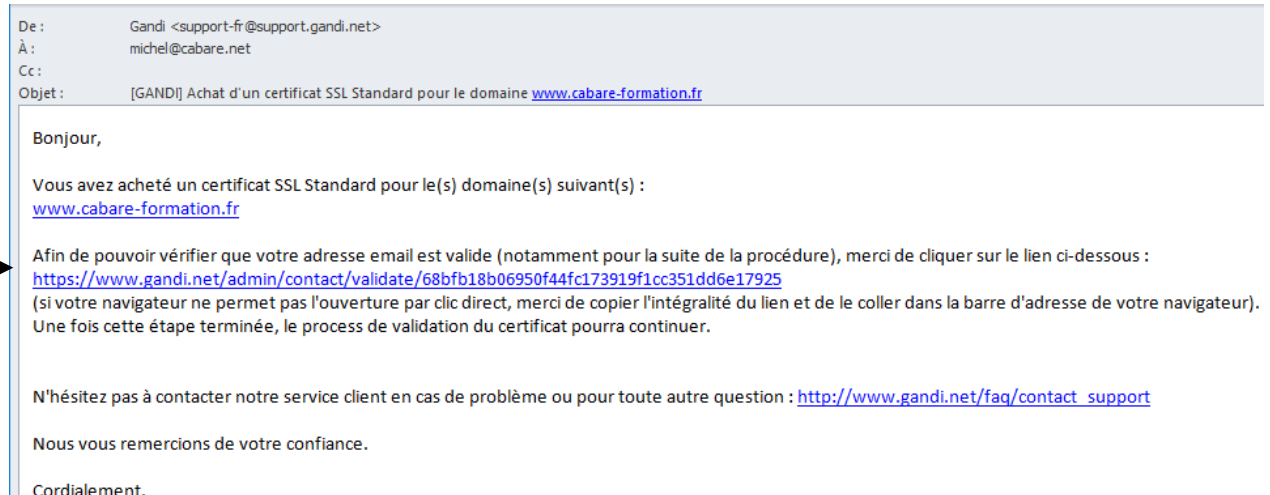
Une fois votre commande validée, en fonction du type de certificat que vous venez d'acheter, vous allez devoir passer un processus de validation.

Vous recevrez un mail vous indiquant les étapes à suivre pour activer votre certificat.

[Accéder à votre compte](#)

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)



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'étape suivante.

et cela déclenche la commande de certificat

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

Filtrer ? [Recherche avancée](#)

Transaction (1/1)	Commande	État	Date de création	
29951651/7	Certificat SSL - Création d'un certificat SSL (cliquez sur le stylo pour un détail 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.

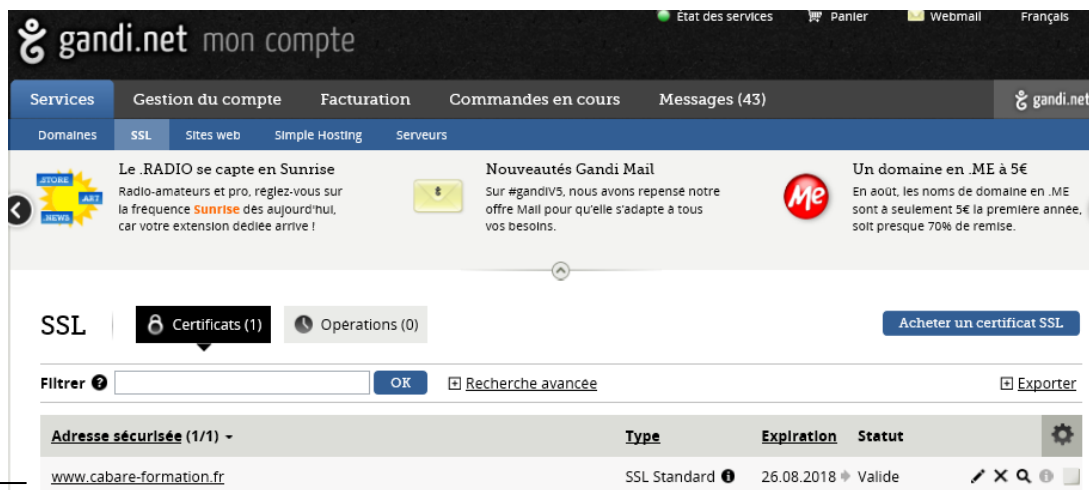
pour une validation par DNS
de modifier la zone DNS de cabare-formation.fr en ajoutant l'enregistrement CNAME qui est communiqué sur l'interface. En cas de certificat Multi-domaines, cette opération est à réaliser pour chaque nom de domaine.

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 créés **Gandi** sont listés sur l'interface, dans l'onglet **SSL**



Lorsque l'on clique dessus, on obtient le détail

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 365 jours)

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

Dernière mise à jour : 25.08.2017

Opérations en cours : 0

[Ajouter une note](#)

[Révoquer de manière définitive](#)

Certificat délivré le : 25.08.2017

[Récupérer](#)

[Télécharger l'intermédiaire](#)

[Régénérer le certificat](#)

Logos (disponibles en 3 langues) : [Récupérer les logos](#)

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

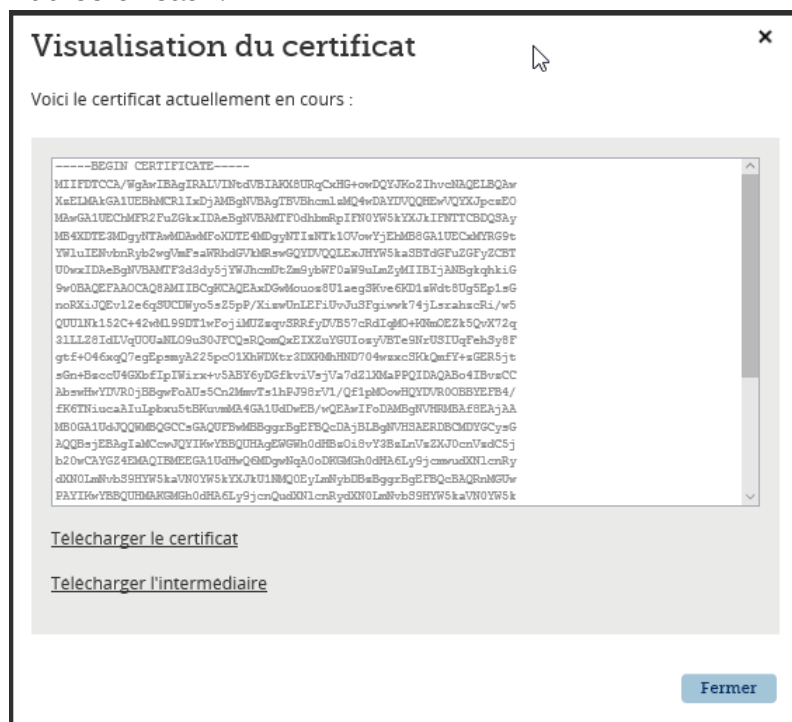
- soit de copier manuellement le certificat crypté à coller dans un fichier texte au format **.crt**

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

....texte crypté...

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

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



```

www.cabare-formation.fr.crt - Bloc-notes
Fichier Edition Format Affichage ?

-----BEGIN CERTIFICATE-----
MIIFDTCCA/WgAwIBAgIRALVNItdVBIAXK8URQcXHG+owDQYJKoZIhvcNAQELBQAw
XzELMAkGA1UEBhMCFR1IcDjAMBAGNVBAGTBVBhcm1zMQ4wDAYDVQQHEWVQYXJpczE0
MAwGA1UEChMFRR2FuZGZkIDAeBgNVBAMTF0dhbmRpfIFN0YW5kYXJkIFNTTCBDQSAy
MB4XDTE3MDgyNTAwMDAwMf0XDTE4MDgyNTIzNTk1OVowYjEhMB8GA1UECzMtYm99t
YWUuIENvbnRyY2wgVmFsaWRhdGVkMRswGQYDVQQLEXJhYW5kaSBTdGFuZGFyZCBT
U0wxIDAeBgNVBAMTF3d3dy5jYWJhcmUtZm9ybWwF0aW9uLmZyMIIBIjANBgkqhkiG
9w0BAQEEFAAOCAQIAMIBGCAQEAxDGwMouoz8U1aegSKve6KD1zWdt8Ug5Ep1sG
noRxiJQEv12e6q5UCDIUy05Z5pP/XizwUnLEFIUvJuSfGfiwwk74jLsrahzcrl/w5
QUU1Nk152C+42wM199D1wFoJiMUZzqvSRRfyDVB57cRdIQMO+KNmOEZk5QvX72q
31LLZ8IdLVqUOUaNL09uS0JFCQsRQomQxEIXZuYGUiozyVBTE9NrUSIUqFehSy8F
gtf+046xqQ7egEpsmyA225pc01XhWDXtr3DXKMhHND704wzxcSKkQmFY+zGER5jt
sGn+BzczU4GXbfIpIWirx+v5ABY6yDGfksiVsjVa7dZ1XMApPQIDAQAB04IBvzCC
AbkwHwYDVR0jBBgwFoAUS5Cn2MmvTs1hPJ98rV1/Qf1pM0owHQYDVR00BBYEFB4/
fK6TNiubcaAtUlpbxu5tBKuvnMA46A1UdDwEB/wQEAwIFoDAMBgNVHRMBAf8EAjAA
MB0GA1UdJQQwMBQGCCcGAQUFBwMBBggrBgEFBQcDAjBLBgNVHSAERDBCMYDGCysG
AQQBsjEBAGIaMCcwJQYIKwYBBQUHAGEWGWh0dHBz0i8vY3BzLnVzZXJ0cnVzdC5j
b20wCAYGZ4EMAQIBMEEGA1UdHwQ6MDgwNqA0oDKGMgh0dHA6Ly9jcmwudXN1cnRy
dXN0LmNvbS5HYW5kaVN0YW5kYXJkU1NMQ0EyLmNybDBzBgggrBgEFBQcBAQRnMGUw
PAYIKwYBBQUHMAKGh0dHA6Ly9jcnQudXN1cnRydXN0LmNvbS5HYW5kaVN0YW5k
YXJkU1NMQ0EyLmNlYyDAI1BggrBgEFBQcAAYYZaHR0cDovL29jc3AudXN1cnRydXN0
LmNvbTA3BgNVHREEMAdAughd3d3cuY2FiYXJ1LWZvcm1hdGlvbi5mcoITY2FiYXJ1
LWZvcm1hdGlvbi5mcjANBgkqhkiG9w0BAQsFAAOCAQEAffJY8FaE0vC0pSqXkynY
r8OLKP2NmG9y50T3/lb1AN5Rf+0b09swu8YS+QAp3FmpUubSIU1+1Wd4+1XEWX2e
Lh01G54C00zrMgUdwctxfDs5j7RJ0csWJRiDB7tKdkfJ0Pvj+1RuW1wrMSFp9M810
JMp/B1QXVGkdq13TzdXvEM2Cz693ptdBtuuTxSBDH9TUyM1j3vNhrSL3zJajX/bo
FMRrYp4hvQCJ03xQ4j3AtSJ4MczJjuGHSOM2qvdVvwqug8EisVviHmzRb/Cv8jLp
7hN73DdZCG030Lq34UJkIRtWL6adIAeWEx3oabp67QP8hXpXkIFbgY+EIHL0/VHP
Sw==

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

```

The screenshot shows a web browser window at the top with the address bar displaying 'Gandi SAS [FR] gandi.net/static/CA5/GandiStandardSSLCA2.pem'. The browser's navigation bar includes links for 'Aiskap Evasion', 'Galerie', 'Le testeur de', and 'Sites suggérés'. The main content area of the browser is mostly obscured by a WordPad application window in the foreground.

The WordPad window is titled 'GandiStandardSSLCA2.pem - WordPad' and shows the 'Affichage' (View) tab. The document content is a certificate file, starting with '-----BEGIN CERTIFICATE-----' and containing a large block of base64-encoded text. The text is partially obscured by a horizontal scrollbar and a vertical scrollbar. The WordPad interface includes a menu bar with 'Fichier' and 'Accueil', a toolbar with various editing tools, and a status bar at the bottom showing 'Presses-papiers', 'Police', 'Paragraphe', 'Insertion', and 'Edition'.

Installation du certificat sur le serveur Linux Simple Hosting

Une fois en possession au minimum

- De la clé privée
- Du certificat SSL

 GandiStandardSSLCa2.pem	26/08/2017 09:09	Fichier PEM
 GandiStandardSSLCa2.txt	26/08/2017 09:12	Document tex
 www.cabare-formation.fr.crt	26/08/2017 09:01	Certificat de s
 www.cabare-formation.fr.csr	25/08/2017 13:27	Fichier CSR
 www.cabare-formation.fr.key	25/08/2017 13:27	Fichier KEY

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

 Sites

Pour savoir **comment lier votre nom de domaine à votre Instance Simple Hosting**, [cliquez ici](#). Si vous souhaitez activer un certificat SSL sur un site (https://), cliquez sur l'icone  ci-dessous.

Adresse (vhost) (20/20)	Création	Statut	
www.formation-grenoble-informatique.com ⓘ	17.06.2015	Actif	  
www.cabare-formation.net ⓘ	18.06.2015	Actif	  
cabare-formation.net ⓘ	18.06.2015	Actif	  
www.cabare-formation.fr ⓘ	17.08.2015	Actif	  
www.cpf-grenoble.com ⓘ	19.08.2015	Actif	  

Activer un certificat

Ajouter un certificat

Pour activer un certificat sur Simple Hosting, il vous faut copier-coller votre certificat ainsi que la clé privée générée lors de l'achat de votre certificat ([voir comment sur notre wiki](#)). À noter que si votre certificat est multi-adresses ou wildcard (multi sous-domaines), l'ensemble des adresses sera sécurisée.

Certificat *

Clé privée *

Copiez ici le contenu de votre clé privée pour qu'elle soit installée sur nos serveurs.

Retour Valider

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

Ajouter un certificat

Pour activer un certificat sur Simple Hosting, il vous faut copier-coller votre certificat ainsi que la clé privée générée lors de l'achat de votre certificat ([voir comment sur notre wiki](#)). À noter que si votre certificat est multi-adresses ou wildcard (multi sous-domaines), l'ensemble des adresses sera sécurisée.

Certificat *

```
-----BEGIN CERTIFICATE-----
MIIFDTCCA/WgAwIBAgIRALVINtDVBIAXK8URqCxHG+owDQYJKoZIhvcNAQELBQAw
XzELMAkGA1UEBhMCFRlIExDjAMBGNVBAgTBVBhcm1zMQ4wDAYDVQQHEWVXYJpczEO
MAwGA1UEChMFMR2FuZGxkIDAeBgNVBAMTF0dhbmRpfIFN0YW5kYXJkeFNTTCBDQSAy
MB4XDTE3MDgyNTAwMDAwMFoXDTE4MDgyNTIzNtk1OVowYjEhMB8GA1UECzMGRG9t
YWluIEIENvbnRyb2wgVmFsaWRhdGVkMRwwGQYDVQLXLEJHYW5kaSBTDGFueGFyZCBT
U0wxIDAEBgNVBAMTF3d3dy5jYWJhcmtUtm9ybwWF0aW9uLmZyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAdGwMouoz8UlaegSKVe6KD1rWdt8Ug5Ep1sG
noRXiJQEv12e6qSUCDWyo5sZ5pP/XizwUnLEf1UvJuSFgiwwk74jLsrzhzcRi/w5
QUUIlnk152C+42wM199DT1wFojiMUZZqvSRRfyDVB57cRdiQMOKNMoeZk5QvX72q

```

Copier ici le certificat (CRT) que vous souhaitez déclarer. Attention : La longueur de la clé doit être de 2048 bits.

Cle privée *

```
-----BEGIN PRIVATE KEY-----
MIIIEvWIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDEMBAYi6jPxTVp
6BIq97ooPXNZ23xSDkSnWwaehFeIlAS+XZ7qpJQInbkjmxnmk/9eLPBScsQJWS8m
SIWCLDCTviMuytqHNxGL/DlBRSU2TXnYL7jbAyX30NPXAWiOIxrNoQ9JFF/INUHn
txFOiow74o2Y4RmTlC9fvareUstnwh0tWpQ5Ro0s725LQkUJCxFciZDEQHdm5gZQ
ijPJUFNF702tRIhSoV6FLLWC1/47jrGpDt6ASmybIDbbmlw7VeFYNe2vcNcoyEc0
PvTjDPFxIgRCZ9j7MYRHmO2waf4HNxxTgzdt8ikhaKVH6/kAFjrIMZ+S+JWyNVrt
1mVcxo89AGMBAAECggEAJcPGvcQCR5QXVv5z2M98hthlrSun34edkXVFdeg9js2o
yBfvsGlJ7VagvztQvgCI7FDMJaKvue+IZv0f8dGdvCKiVRR5AgQInaB8SOMNaal6
JbHx7D5r5YrN7Bn6TTnVaJVOPiXslfxibL7hXkr4/+HSDY9uw+iHQe+ZX1gijSMK

```

Copiez ici le contenu de votre clé privée pour qu'elle soit installée sur nos serveurs.

Désormais le certificat est activé :



Sites

Pour savoir **comment lier votre nom de domaine à votre instance Simple Hosting**, [cliquez ici](#). Si vous souhaitez activer un certificat SSL sur un site (https://), cliquez sur l'icône  ci-dessous.

Adresse (vhost) (20/20)	Création ▾	Statut	
www.formation-grenoble-informatique.com ⓘ	17.06.2015	Actif	  
www.cabare-formation.net ⓘ	18.06.2015	Actif	  
cabare-formation.net ⓘ	18.06.2015	Actif	  
www.cabare-formation.fr ⓘ	17.08.2015	Actif	  
www.cpf-grenoble.com ⓘ	19.08.2015	Actif	  

 Désactiver ce certificat

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]

 .htaccess - Bloc-notes

Fichier Edition Format Affichage ?

RewriteEngine On

RewriteCond %{SERVER_PORT} 80

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

Redirection http + https de domaine sur [www.domaine](http://www.cabare-formation-informatique.net) (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 créé 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)

 .htaccess - Bloc-notes

Fichier Edition Format Affichage ?

RewriteEngine On

RewriteCond %{SERVER_PORT} 80

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

ou encore d'une autre manière

#RewriteRule ^(.*)\$ https://www.cabare-formation-informatique.net/\$1 [QSA,L,R=301]

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-informatique.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

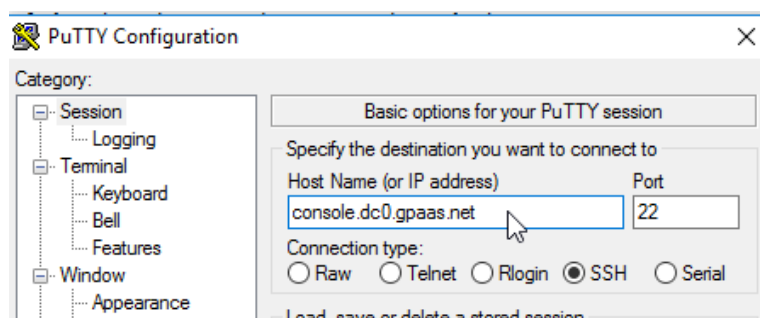
On doit faire la demande **CSR** depuis le serveur **Gandi Simple Hosting** sur lequel on souhaite installer le certificat à travers une **console SSH** (permettant ensuite de passer la commande OpenSSL, mais aussi toutes les commandes souhaitées d'ailleurs)

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.

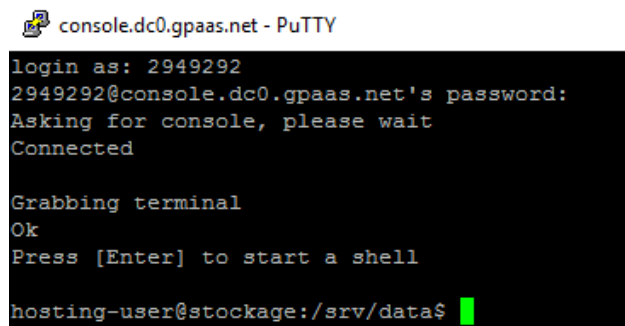
Lancement console SSH

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 à atteindre

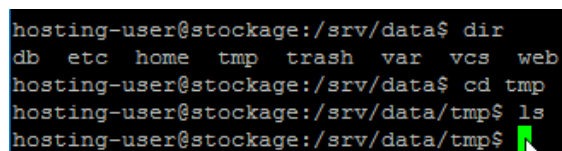


et pour stockage ce sera login **2949292** mdp **Gandistockzk28**



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

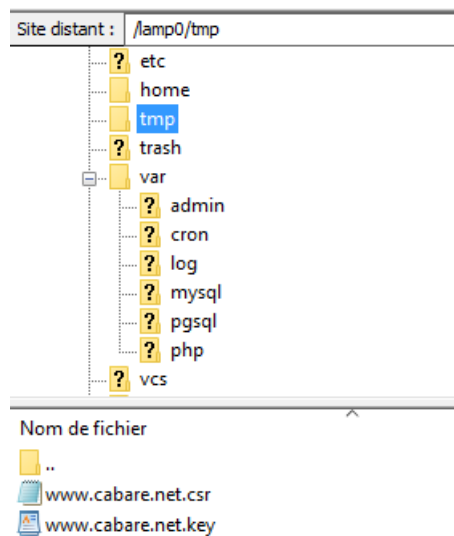
```
An optional company name []:
```

Optionnel

A la fin de la commande on obtient 2 fichiers, créés 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 vérifier 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

 thawteDVSSLCA-G2.cer	29/08/2017 09:31	Certificat de s
 thawtePrimaryRootCA.cer	29/08/2017 09:31	Certificat de s
 www.cabare.net.cer	29/08/2017 09:31	Certificat de s

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

 intermediaire+racine.pem
 racine+intermediaire.pem
 www.cabare.net.p7b

Installation du certificat sur le serveur Linux Simple Hosting

Une fois en possession au minimum

- De la clé privée
- Du certificat SSL

 thawteDVSSLCA-G2.cer	29/08/2017 09:31	Certificat de s
 thawtePrimaryRootCA.cer	29/08/2017 09:31	Certificat de s
 www.cabare.net.cer	29/08/2017 09:31	Certificat de s
 www.cabare.net.csr	26/08/2017 12:26	Fichier CSR
 www.cabare.net.key	26/08/2017 12:26	Fichier KEY

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

 Sites

Pour savoir **comment lier votre nom de domaine à votre instance Simple Hosting**, [cliquez ici](#). Si vous souhaitez activer un certificat SSL sur un site (https://), cliquez sur l'icone  ci-dessous.

Adresse (vhost) (6/6)	Création	Statut	
ccb805f0f1.url-de-test.ws 	02.02.2015	Actif	  
www.cabare-formation-informatique.net 	14.08.2015	Actif	  
www.cabare-formation-internet.net 	15.08.2015	Actif	  
www.cabare-formation-windows.net 	15.08.2015	Actif	  
www.cabare.net 	16.08.2015	Actif	  
perso.cabare.net 	17.08.2015	Actif	  

Activer un certificat

Ajouter un certificat

Pour activer un certificat sur Simple Hosting, il vous faut copier-coller votre certificat ainsi que la clé privée générée lors de l'achat de votre certificat ([voir comment sur notre wiki](#)). À noter que si votre certificat est multi-adresses ou wildcard (multi sous-domaines), l'ensemble des adresses sera sécurisé.

Certificat *

Copier ici le certificat (CRT) que vous souhaitez déclarer. Attention : La longueur de la clé doit être de 2048 bits.

Clé privée *

Copiez ici le contenu de votre clé privée pour qu'elle soit installée sur nos serveurs.

[Retour](#) [Valider](#)

ANNEXE1 : TYPE & CONVERSION 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

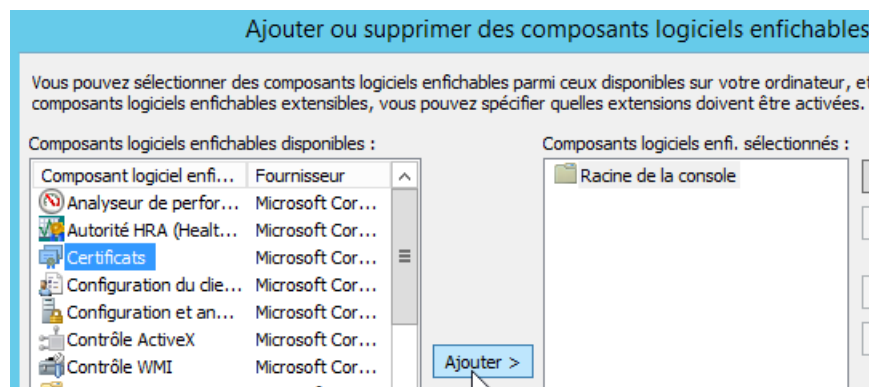
Il est possible de récupérer le certificat posé sur le serveur IIS via

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

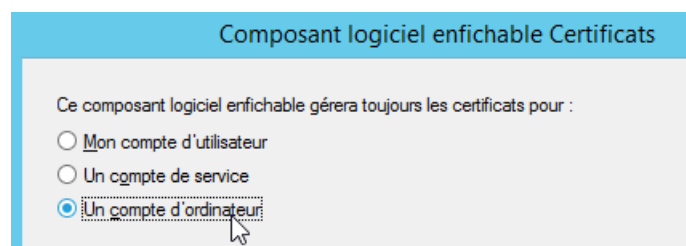
Méthode Serveur Windows vers pfx

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

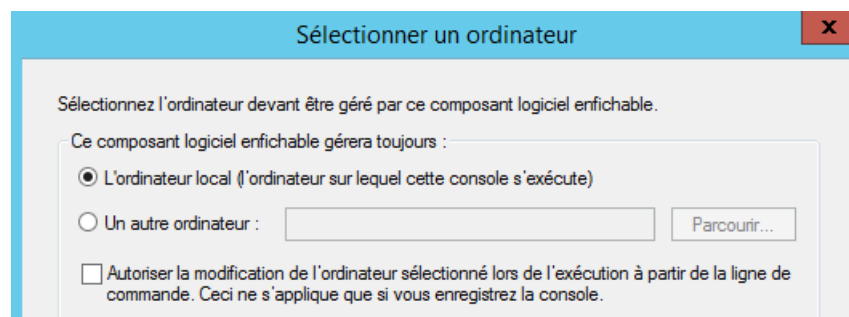
Mmc puis **ajout suppression de composant logiciels enfichable / certificats**

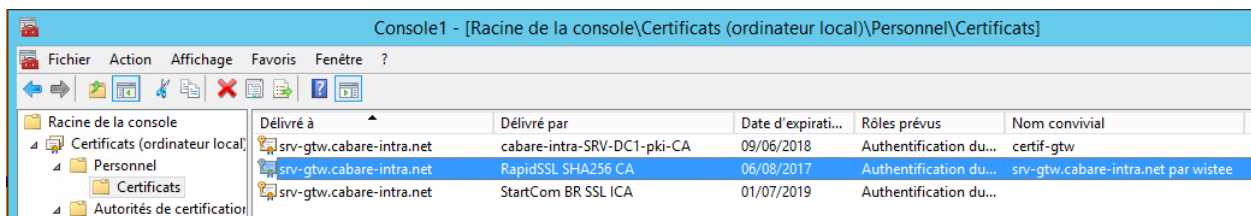


On demande **un compte d'ordinateur**

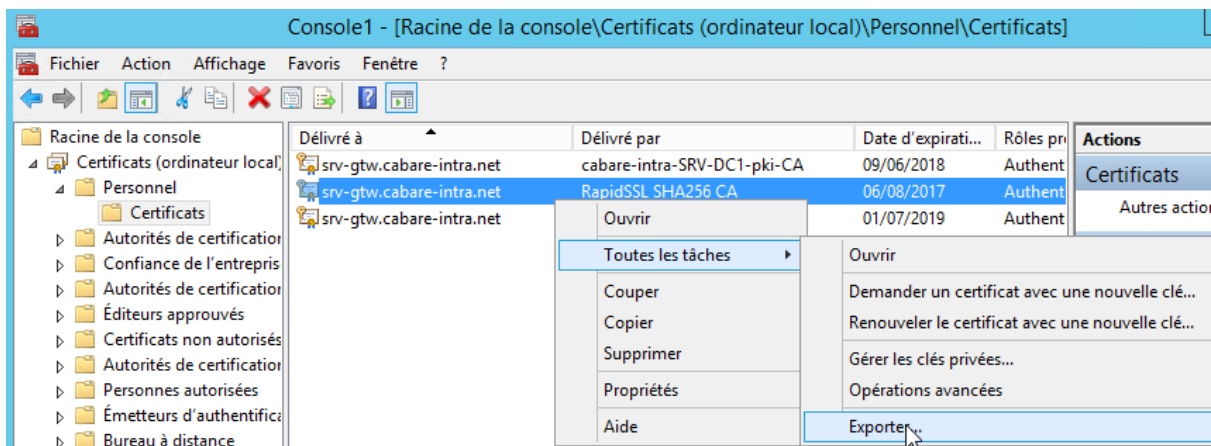


L'ordinateur local





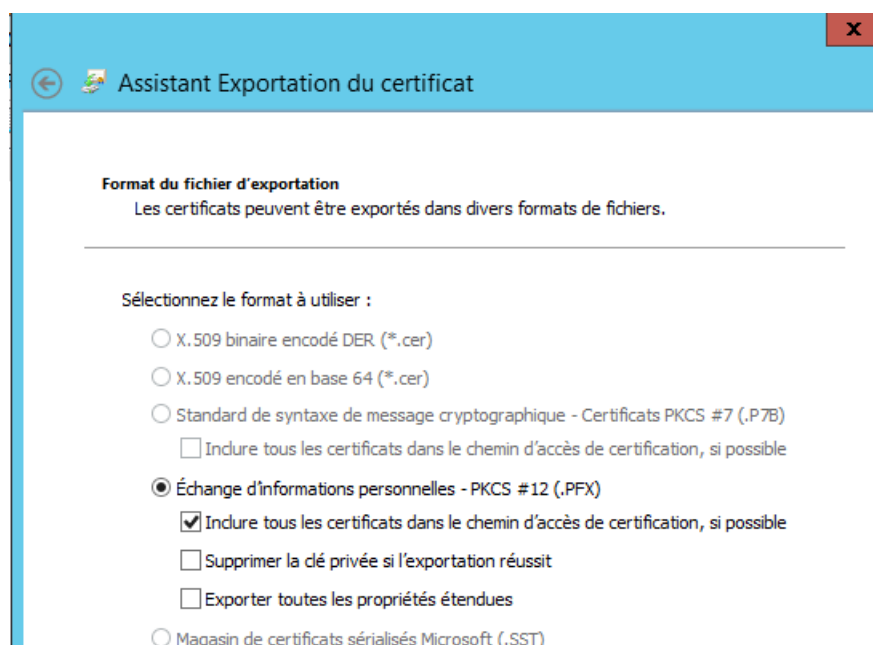
Après avoir sélectionné notre certificat, on demande via clic droit / **exporter**



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

 mot de passe certificat pfx = sslzk28.
 srv-gtw.cabare-intra.net.pfx

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...

 GeoTrustGlobalCA.cer
 RapidSSLSHA256CA.cer
 srv-gtw.cabare-intra.net.cer

.CER vers .PFX : Convertir un certificat au format .CER vers le format .PFX (PKCS#12) avec OpenSSL :

```
openssl pkcs12 -in certificat-ssl.cer -certfile cert-intermediaire.cer -certfile cert-racine.cer -inkey cle-privee.key -export -out certificat-ssl.pfx
```

Bonjour,

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

Cordialement,

ANNEXE3 : CONSOLE SSH GANDI SUR SIMPLE HOSTING

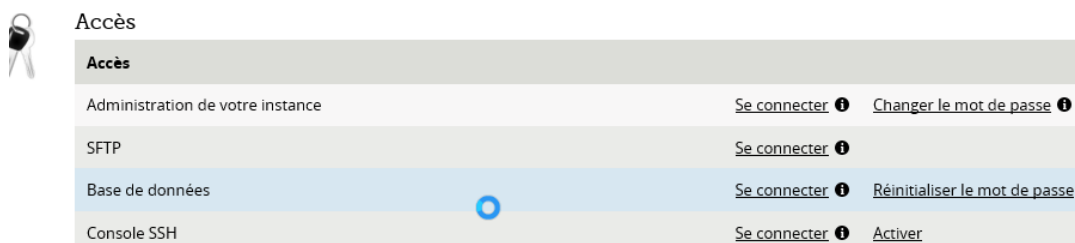
Console SSH et Putty

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.

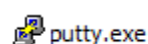
Console putty



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



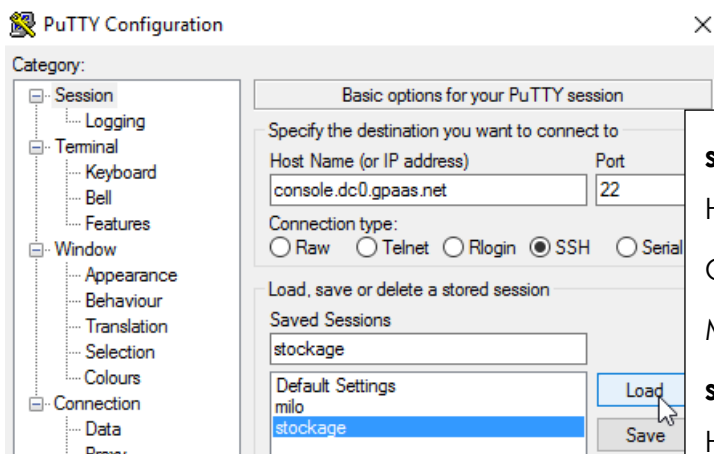
donc



01/07/2013 07:21

Application

472 Ko



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**)

console.dc0.gpaas.net - PuTTY

```
login as: 3802978
```

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

console.dc0.gpaas.net - PuTTY

```
login as: 3802978
```

```
3802978@console.dc0.gpaas.net's password:
```

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

console.dc0.gpaas.net - PuTTY

```
login as: 3802978
```

```
3802978@console.dc0.gpaas.net's password:
```

```
Asking for console, please wait
```

```
Connected
```

```
Grabbing terminal
```

```
Ok
```

```
hosting-user@milo:/srv/data$
```

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
```