

Demande et installation d'un certificat

Table des matières

ntroduction	2
inux	3
Demander un certificat	3
Installer un certificat	6
Récupérer la clé privée	6
Nindows	7
Demander un certificat	7
Installer un certificat	10
Récupérer la clé privée 1	12

Introduction

Pour obtenir un certificat, il faut dans un premier temps générer une demande de certificat (CSR, Certificate Signing Request). Lors de la demande de certificat vous allez générer une clé privée. Dès que cette clé est générée, faites-en une copie de sauvegarde et protégez-la très sérieusement (voir la partie « **Récupérer la clé privée** »). Le CSR contient la clé publique et des informations d'identification du demandeur que l'on spécifiera dans la documentation ci-dessous.

Linux

Demander un certificat

- Pour commencer, vérifier si « openssl » est bien installé sur votre système qui héberge le service
- Ensuite ouvrez un terminal, allez dans le répertoire « certificats » du service (ex : service Apache) que vous désirez mettre en place et tapez la commande suivante :
 - Cas d'un certificat avec un seul domaine

openssl req -newkey rsa:4096 -keyout nomservice.universite-paris-saclay.fr.key -nodes
-subj "/C=FR/O=UNIVERSITE PARIS-SACLAY/CN=nomservice.universite-parissaclay.fr/" -out nomservice.universite-paris-saclay.fr.csr

Attention, nomservice.universite-paris-saclay.fr devra correspondre au nom DNS du service

Exemple : pour le service d'annuaire Adonis (<u>https://adonis.universite-paris-saclay.fr</u>), le nom DNS a renseigné est adonis.universite-paris-saclay.fr

> La demande de certificat est alors générée voir ci-dessous

- Cas d'un certificat avec des multi-domaines
- En ligne de commande :

Vous devez vous assurer que le fichier de configuration openssl par défaut existe. Pour cela, tapez la commande :

Is `openssI version -d | awk -F"" '{print \$2}''/openssI.cnf

Si le fichier openssl.cnf est /etc/pki/tls/openssl.cnf et le nom des services sont nomservice.universite-paris-saclay.fr et nomservice.u-psud.fr, tapez la commande :

openssl req -newkey rsa:4096 -keyout nomservice.universite-paris-saclay.fr.key -nodes
-subj "/C=FR/O=UNIVERSITE PARIS-SACLAY/CN=nomservice.universite-parissaclay.fr/" -reqexts SAN -config <(cat /etc/pki/tls/openssl.cnf <(printf
"\n[SAN]\nsubjectAltName=DNS:nomservice.universite-paris-saclay.fr,DNS: nomservice.upsud.fr")) -out nomservice.universite-paris-saclay.fr.csr</pre>

• En utilisant un script dont il faudra modifier les variables :

Vous pouvez télécharger le script à l'adresse : .<u>https://securite-informatique.dsi.universite-</u> paris-saclay.fr/docs/download/CreationCSR.sh

#!/bin/sh

```
# Initialisation des variables
hostname="monservice.universite-paris-saclay.fr"
alternative_name="monservice.universite-paris-saclay.fr monservice.u-psud.fr"
organisation="UNIVERSITE PARIS-SACLAY"
# On cherche le fichier par défaut pour openSSL
def=`openssl version -d | awk -F'"' '{print $2}'`
#On le copie en local en activant l'extension v3_req.
cat $def/openssl.cnf | sed 's/^#[ ]*req_extensions = v3_req/req_extensions =
v3_req/' | sed 's/\[ v3_req \]/\[ v3_req \]\'$'\nsubjectAltName = @alt_names/' >
./openssl.cnf
#On ajoute la section [ alt_names ]
echo "[ alt_names ]" >> ./openssl.cnf
#On ajoute tous les noms de $alternative_name
count=0
```

```
for i in $alternative_name; do
    let count="$count +1"
        echo "DNS.$count=$i" >> ./openssl.cnf
done
#On génère les fichiers .key et .csr
openssl req -config ./openssl.cnf -newkey rsa:4096 -out $hostname.csr -keyout
$hostname.key -nodes -subj "/C=FR/O=$organisation/CN=$hostname/"
#On peut controler les noms inclus avec la commande ci-dessous
#openssl req -text -noout -in $hostname.csr
```

Copiez et collez le contenu du script dans un fichier.sh. Rendre ce script exécutable (chmod a+x script.sh) Exécutez le script : ./script.sh

- La clé privée « nomservice.universite-paris-saclay.fr.key » et la demande de certification « nomservice.universite-paris-saclay.fr.csr » sont maintenant créés dans le répertoire « certificats »
- Envoyer la demande de certificat (CSR) au pôle « sécurité » de la Direction des Systèmes d'Information via la plateforme <u>https://sos.di.u-psud.fr</u> Catégorie « Sécurité » afin qu'il puisse générer un certificat.

Attention, il faut envoyer la demande avec les lignes « Begin New Certificate Request » et « End New Certificate Request ».

De plus, indiquez avec l'envoi du CSR, le service utilisé qui se rapproche le plus de la liste ci-dessous

Apache Microsoft IIS 5 or 6 Microsoft IIS 7 Microsoft IIS 8 Microsoft Exchange Server 2007 Microsoft Exchange Server 2010 Microsoft Exchange Server 2013 Torncat Microsoft Lync Server 2010 Microsoft Lync Server 2013 Microsoft Office Communications Server 2007 Microsoft Live Communications Server 2005 IBM HTTP Server Netscape iPlanet Java Web Server (Javasoft / Sun) certificat Lotus Domino Microsoft IIS 1.x to 4.x

Netscape Enterprise Server Novell NetWare Oracle SunOne Qmail Juniper F5 FirePass F5 Big-IP Cisco WebStar Bea Weblogic 7 and older Zeus Web Server Citrix (Other) Barracuda BEA Weblogic 8 & 9 cPanel Lighttpd

nginx Citrix Access Essentials Microsoft Exchange Server 2003 Mac OS X Server Citrix Access Gateway 4.x Citrix Access Gateway 5.x and higher Microsoft OCS R2 Microsoft Small Business Server 2008 & 2011 Novell iChain Microsoft Forefront Unified Access Gateway OTHER La Direction des Systèmes d'Information vous enverra ensuite un fichier zip qui contiendra le certificat (nomservice_universite-paris-saclay_fr.cer) ainsi qu'un fichier donnant des instructions pour l'installation si besoin.

Installer un certificat

Pour l'installation du certificat sous Linux, rechercher sur Internet comment installer un certificat pour le service que vous désirez mettre en place. Vous pouvez également vous aider des instructions envoyées dans le fichier zip.

Récupérer la clé privée

Pour récupérer la clé privée, il suffit de récupérer le fichier « nomservice.universiteparis-saclay.fr.key », le crypter et le copier dans un endroit sécurisé.

Windows

Demander un certificat

Pour créer cette demande il faut télécharger l'outil suivant via ce lien <u>https://securite-informatique.dsi.universite-paris-saclay.fr/docs/download/DigiCertUtil.exe</u>. Une fois l'exécutable lancé sur le serveur, suivre les étapes suivantes :

> Cliquer sur « SSL » à gauche de la fenêtre et sur « Create CSR »



> Sélectionner « **SSL** » et renseigner les champs suivants

🜀 DigiCert Certificate Utility for Windows©

Create CSR

Certificate Det	ails		Information
Certificate Type:	● SSL ○ Code Signing		Key Size
Common Name:	nomservice.universite-paris-saclay.fr		Kay sizes amaller than 2049 are considered
Subject Alternative Names:	nomservice.universite-paris-saclay.fr nomservice.u-psud.fr	~	ney sizes smaller than 2048 are considered insecure.
Organization:	Université Paris-Saday		
Department:			
City:	Orsay		
State:		~	
Country:	France	\sim	
Key Size:	4096	\sim	
Provider:	Microsoft RSA SChannel Cryptographic Provider	\sim	
	Generate Cancel		

« **Common Name** » : Saisir le nom DNS du service (exemple : service d'annuaire Adonis <u>https://adonis.universite-paris-saclay.fr</u>, le nom sera adonis.universite-paris-saclay.fr)

- « Subject Alternative » : Saisir les autres domaines si vous en avez
- « Organization » : Saisir le nom de l'établissement « Université Paris-Saclay »
- « City » : Entrer la ville où se situe l'établissement
- « Country » : Entrer le pays
- « Key Size » : Définir la taille de la clé à 4096
- « **Provider** » : Sélectionner l'algorithme de cryptage « **Microsoft RSA SChannel Crytographic Provider** »

 \times

The certificate request has been successfully created.	
BEGIN NEW CERTIFICATE REQUEST	_
MIIFDTCCAvUCAQAwbzELMAkGA1UEBhMCR1IxDjAMBgNVBAcTBU9yc2F5MSAwHgYD	
VQQKExdVbml2ZXJzaXTpoJBhcmlzLVNhY2xheTEuMCwGAlUEAxM1bm9tc2Vydmlj	
ZS51bml2ZXJzaXR1LXBhcmlzLXNhY2xheS5mcjCCAiIwDQYJKoZIhvcNAQEBBQAD	
ggIPADCCAgoCggIBAPB521MXwv/OYQb+PndKKzcNVt52JiCfbUhiPmEFq2v+e1N7	
cfS2+E6Hg1MdJBsbVyTQFKz2Q6jAn008VPQ8Q1n5Aw9b9X1MUeyD5Zo1DVoPaegm	
YekgPnx0guugx0eoi2wUSge90xhzxDtUFXgd21TeEMSGtijxiSdYq6nvE2f0tdmh	
7sqrImC1BHG2H7oS1nqY51pxJc6x1NNTQPcY+13+RSb14ZbSeq/XCxuTuf5TxWRF	
bA/f6kND1Wm+HLAIA1pckeLSQtr86UHok+x9Se3MaceBe0LbhY7ckH4ogfFtEc9v	
jpqOWMijDLVYP/kwLRRj5ifA4kaVn+VctpJ82Lb1wXynHPkympCuzHB9VHhyi0WV	
0c5QiSkYakJp0fFywcaGqAjiUarFZMTBNK77KSOm0BBmEKjbMnGK3hNPN+huUrX1	
fxA9WLF11Qvhgva+K0tWEK1wssD8MJs0BnpPxmoxdDw04J01Uj7efPXRSeCzwiDb	
6VfAPDD0Z3xHQ1XeU5Hzj6qp6wIUZoKqw2/OgZYAzVyV8AitL15khA/QIaHdzFR/	
6xN9kyWhTf+Xip+uH9qpi+Ta2OpcvQEKQOop/fF4ylLc9WdGyl6UJ74O/TRqx5ay	
rlwC/4B6w/UfMgZIXoktPnlxfshvuKBqe9YCaOF1Nto77/4BXFI1GU+CBSrdAgMB	
AAGgWTBXBgkqhkiG9w0BCQ4xSjBIMEYGA1UdEQQ/MD2CJW5vbXN1cnZpY2UudW5p	
dmVyc210ZS1wYXJpcy1zYWNsYXkuZnKCFG5vbXN1cnZpY2UudS1wc3VkLmZyMA0G	
CSqGSIb3DQEBBQUAA4ICAQDgCJVK/M+oXWFefNxbxoQYpHUnaWj03o9fTw02dgog	
B8gHo4h/1PE0XaYFOOD+X8B7Ag+Vm+JCvvkk8Z1BHN/ZXeqG1+kjk0Cm8CFZ5m3B	
Ylnim4xWprPXvzelvs716jAWpF2OYn16hbBdZbb+Nqh1vyK3iFt7iC2XLvu1S8+k	
Dqu7FlxrucZd2jk8s7MEBWUgNVHR6srsVPPawkTsCiKRH48LNtnzaq+RNX6upKwD	
yunIFqg2ZBiW4N67USxc0R2z0+fHgaj7/WMgkJ4vFHL52Pi1TnN64RtGLcXxeoTx	
QH5Q0e72EPG6JNBIrJ322EVNq8n4hFqKp/phNPwmWG0XcifN1HiOm0SjAF3vtUG1	

Copiez la demande de certificat (CSR) et l'envoyer au pôle « sécurité » de la Direction des Systèmes d'Information via la plateforme <u>https://sos.di.u-psud.fr</u> Catégorie « Sécurité » afin qu'il puisse générer un certificat.

Attention, il faut envoyer la demande avec les lignes « Begin New Certificate Request » et « End New Certificate Request ».

De plus, indiquez avec l'envoi du CSR, le service utilisé qui se rapproche le plus de la liste ci-dessous et précisez dans votre demande qu'il s'agit d'un certificat de type multi-domaines.

Apache	
Microsoft IIS 5 or 6	
Microsoft IIS 7	
Microsoft IIS 8	
Microsoft Exchange Serv	ver 2007
Microsoft Exchange Serv	ver 2010
Microsoft Exchange Serv	ver 2013
Tomcat	
Microsoft Lync Server 20	010
Microsoft Lync Server 20	013
Microsoft Office Commu	inications Server 2007
Microsoft Live Communi	ications Server 2005
IBM HTTP Server	
Netscape iPlanet	
Java Web Server (Javasof	t/Sun)
Lotus Domino	certificat
Microsoft IIS 1.x to 4.x	

Netscape Enterprise Server Novell NetWare Oracle SunOne Qmail Juniper F5 FirePass F5 Big-IP Cisco WebStar Bea Weblogic 7 and older Zeus Web Server Citrix (Other) Barracuda BEA Weblogic 8 & 9 cPanel Lighttpd

nginx Citrix Access Essentials Microsoft Exchange Server 2003 Mac OS X Server Citrix Access Gateway 4.x Citrix Access Gateway 5.x and higher Microsoft OCS R2 Microsoft Small Business Server 2008 & 2011 Novell iChain Microsoft Forefront Unified Access Gateway OTHER La Direction des Systèmes d'Information vous enverra ensuite un fichier zip qui contiendra le certificat (nomservice_universite-paris-saclay_fr.cer) ainsi qu'un fichier donnant des instructions pour l'installation si besoin.

Installer un certificat

- Lorsque vous avez récupéré le certificat, vous pouvez l'installer sur le serveur à l'aide de l'outil « DigiCertUtil.exe ».
- > Cliquez sur « SSL » à gauche de la fenêtre puis sur « Import » en haut à droite

🚺 DigiCert Cer	tificate Utility for Windows	0				- • •
Ødig	jicert [®] CER	RTIFICATE UTILITY ;	for Windows°	\$ 1.80 (support@di).896 gicert.com	.7973 Live Chat
	SSL Certificates			Create CSR	1 Import	C Refresh
	Issued To	Expire Date	Serial Number	Friendly Name	Issuer	
SSL						
Code Signing						
X						
Tools						
0						
Account						_
Version 2.3.7						Close

Cliquez sur « Browse » pour allez chercher le certificat et cliquez sur « Suivant » comme ci-dessous

🚺 DigiCert Certificate Utility for Windows©	×
Certificate Import	
This wizard will assist you with importing a certificate. Depending on the type of file you are importing you may be prompted for a password to decrypt the private key.	
c:\Users\User\nomservice_universite-paris-saclay_fr Browse	
< Précédent Suivant > Annuler	

Ensuite entrer la valeur de « Name : » dans le champ « Enter a new friendly name.. » si ce champ est vide puis cliquer sur « Terminer »

0	DigiCert Certificate Utility for Windows©	٤
Certific	ate Import	
The following o the certificate Name: Serial Number: Thumbprint: Private Key:	ertificate is ready to be imported. For more details of press the View Certificate button. officewebtest.ups.u-psud.fr 044A78AC0CFAE59B1F1212A4CB481470 9F6E9FD3E17697DE640D9AFB90CC5966FF877F01 Search for an existing private key match on the computer	50 St.
officewebtes Press the Finis	h button to import the certificate and search for a matching private key.	
	< Back Finish Cancel]

🜀 DigiCert Certificate Utility for Windows©	×
Certificate Import	
The following certificate is ready to be imported. For more details of the certificate press the View Certificate button. Name: stream.dsi.universite-paris-saclay.fr Serial Number: 0AAA7373D31B556280CCB44B2AA19942 Thumbprint: CB224FC362DF605A68D27088035F410E21C9D24A Private Key: Search for an existing private key match on the computer Enter a new friendly name or you can accept the default:	cate
nomservice.universite-paris-saday.fr	
Press the Finish button to import the certificate and search for a matching private key.	
< Précédent Terminer Annu	ler

Récupérer la clé privée

Cliquer sur « Démarrer » et lancer la commande « mmc.msc » dans la zone de recherche. Il faut exécuter « mmc.msc » en mode administrateur.

	Ouvrir	
Fic 殿	Exécuter en tant qu'administrateur	_
1	Edit with Notepad++	
9	AxCrypt	F
×	Rechercher des virus	
×	Placer en quarantaine	
	Restaurer les versions précédentes	
	Envoyer vers	- F
	Couper	
	Copier	
	Supprimer	
	Ouvrir l'emplacement du fichier	
	Propriétés	
_		
•	plus do résultats	

> Ajouter un composant logiciel enfichable



Sélectionner « Certificats » et cliquer sur « Ajouter »

	nea diaportionea .			Composants logiciels entil selection	ines :
omposant logiciel enfi	Fournisseur	-		Racine de la console	Modifier les extensions
Analyseur de perfor	Microsoft Cor Microsoft Cor	ш			Supprimer
Configuration du clie	Microsoft Cor				Monter
Controle ActiveX	Microsoft Cor	-0.18			Descendre
	Microsoft Cor		Ajouter >		A
Dossier	Microsoft Cor				
Dossiers partagés	Microsoft Cor				
Éditeur d'objets de s	Microsoft Cor				
Éditeur d'obiets de s	Microsoft Cor				
Éditeur de gestion d	Microsoft Cor				
Gestion de l'impression	Microsoft Cor				August
i					Avance

Sélectionner « Compte ordinateur »



> Sélectionner ensuite « ordinateur local »

Sélectionnez l'ordinateur de Ce composant logiciel enfi	evant être géré par ce composant logiciel enfichable. Tichable gérera toujours :
L'ordinateur local (l'ord Un autre ordinateur :	dinateur sur lequel cette console s'exécute)
Autorise <u>r</u> la modificati commande. Ceci ne s	ion de l'ordinateur sélectionné lors de l'exécution à partir de la ligne de s'applique que si vous enregistrez la console.

> Chercher votre certificat installé et cliquer sur « exporter »



La fenêtre « Assistant d'exportation de certificat » s'ouvre, cliquer sur « suivant ». > Si la clé privée est exportable, sélectionner « oui, exporter la clé privée »

ssistant exportation de certificat		
Exportation de la clé privée		
Vous pouvez choisir d'exporte	r la dé privée avec le certificat.	
Les d <mark>és privées sont protégée</mark> avec le certificat, vous devrez	es par mot de passe. Pour pouvoir exporter la d z entrer un mot de passe.	lé privée
Voulez-vous exporter la clé pr	ivée avec le certificat ?	
Oui, exporter la dé pri	ivée	
🔘 Non, ne pas exporter	la dé privée	
Informations sur <u>l'exportation des r</u>	<u>dés privées</u>	
		Ann

> Sélectionner « Echange d'informations personnelles »

Format de fichier d'exportation Les certificats peuvent être exportés sous plusieurs formats de fichier.	
Sélectionnez le format à utiliser :	
🔘 X.509 <u>b</u> inaire encodé DER (.cer)	
🔘 <u>X</u> .509 encodé en base 64 (.cer)	
🔘 Standard de syntaxe de message de chiffrement - Certificats PKCS #7 (.p7b)	
Inclure tous les certificats dans le chemin d'accès de certification si possible	2
Echange d'informations personnelles - PKCS #12 (.pfx) Inclure tous les certificats dans le chemin d'accès de certification si possible	2
Supprimer la dé privée si l'exportation s'effectue correctement	
Exporter toutes les propriétés étendues	
Magasin de certificats sérialisés Microsoft (.sst)	
Informations sur les <u>formats de fichiers de certificats</u>	
< Précédent Suivant >	Annuler

> Définir un « mot de passe » pour protéger la clé privée

t de passe	
Pour maintenir la sécurité, vous o passe.	devez protéger la clé privée en utilisant un mot de
Entrez et confirmez le mot de pas	sse.
Mot de passe :	
••••	
Entrer puis confirmer le mot d	le passe (obligatoire) :
••••	

> Cliquer sur « Parcourir » afin de sauvegarder cette clé privée

stant Exportation de certificat		
ichier à exporter Spécifiez le nom du fichier à exporter		
Nom du fichier :		12.
C: \Users \User \Desktop \clé_privée.pfx	Parcouri	r

> Puis cliquer sur « Terminer »