



CRIAÇÃO E RENOVAÇÃO DE CERTIFICADOS

VERSÃO 1

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
23/04/2020	1	Criação do manual	Fábio Abreu

ACRÓNIMOS, TERMOS E DEFINIÇÕES

Sigla	Definição

Índice

1.	Introdução	4
2.	Programas a instalar	5
3.	Criar certificado inicial	6
3.1	Detalhes	6
3.2	Verificação	7
3.3	Criar ficheiros	9
3.3.1	Keystore.JKS	9
3.3.2	Certificado .PFX	10
3.3.3	Criar CRT e KEY	10
4.	Renovar certificados	11
4.1	Colocação e renovação dos ficheiros	11
5.	Conclusão	12

1. INTRODUÇÃO

Para a disponibilização de serviços web de uma forma segura é necessário o uso de certificados SSL válidos, existe uma ferramenta que permite a criação desses certificados de uma forma gratuita com uma validade de 3 meses.

O objetivo deste manual é consolidar o conhecimento adquirido na criação de certificados pelo site LetsEncrypt ZeroSSL e posteriormente a sua automatização pelo uso da linha de comandos em sistemas Windows.

2. PROGRAMAS A INSTALAR

Para podermos seguir todos os passos deste manual sem nada falhar, existem alguns programas que devem estar pré-instalados:

➤ Java

- Versão de 64 bits:

https://javadl.oracle.com/webapps/download/AutoDL?BundleId=242060_3d5a2bb8f8d4428bbe94aed7ec7ae784

- Versão de 32 bits:

https://javadl.oracle.com/webapps/download/AutoDL?BundleId=242058_3d5a2bb8f8d4428bbe94aed7ec7ae784

➤ OpenSSL

- Versão de 64 bits: https://indy.fulgan.com/SSL/openssl-1.0.2u-x64_86-win64.zip

- Versão de 32 bits: <https://indy.fulgan.com/SSL/openssl-1.0.2u-i386-win32.zip>

➤ ZeroSSL Portable Client

- Versão de 64 bits:

<https://github.com/do-know/Crypt-LE/releases/download/0.35/le64.zip>

- Versão de 32 bits:

<https://github.com/do-know/Crypt-LE/releases/download/0.35/le64.zip>

Apenas o Java tem de ser instalado. O OpenSSL e o ZeroSSL não necessitam de instalação e os ficheiros binários (.exe) estão prontos a ser usados após o download.

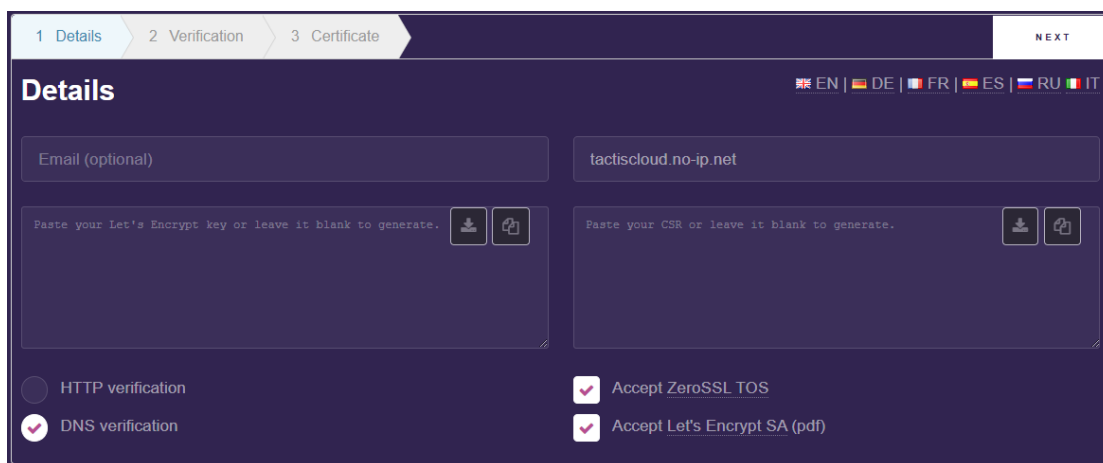
3. CRIAR CERTIFICADO INICIAL

De momento os certificados iniciais utilizados pela Tactis já existem, e o único processo utilizado é o de renovação dos mesmos. No entanto é sempre bom saber como é que as coisas que já existem foram feitas.

3.1 DETALHES

Para criar os ficheiros iniciais devemos dirigir-nos a <https://zerossl.com/free-ssl/#crt>

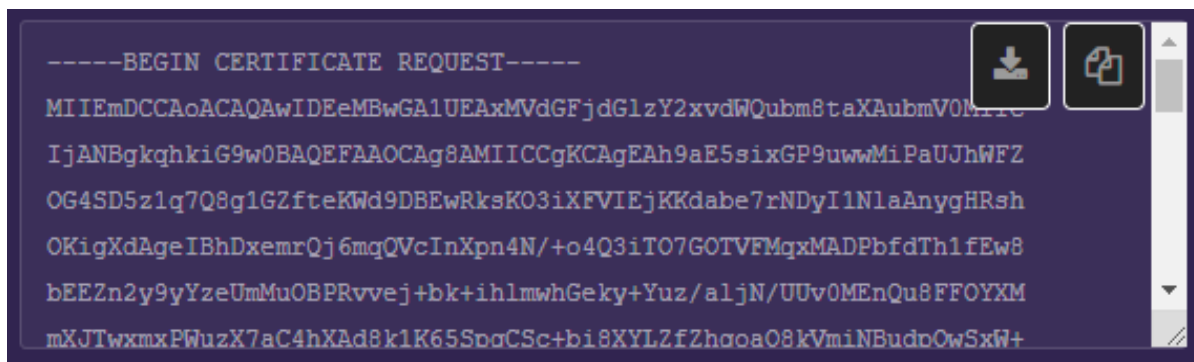
Aqui vamo-nos deparar com uma página que deve ser preenchida da seguinte maneira:



Como na imagem, devemos escrever o nosso nome de domínio (tactiscloud.no-ip.net) onde diz "Domains", e seleccionar ambos os "Accept" e "DNS Verification" e clicar NEXT.

Ao clicar em NEXT vamos receber a mensagem: "Include www-prefixed version too?", devemos responder NO.

Após alguns segundos, vai aparecer alguma informação no campo de texto da direita:



Devemos guardar esta informação - chamada domain-csr - como ficheiro, para tal basta clicar no primeiro botão (que tem uma seta a apontar para um disco). A seguir ao download basta clicar em NEXT outravez.

Após alguns segundos vai aparecer alguma informação no campo de texto da esquerda:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEKAAIBAAKCAgEAidb7gJZ2AekgNTDkngzi1EN59DuEvd72mAb4ma5eU0z0...
FIs70cZVZHaCCOuNy7G9n/4+9G4+EHsKJpCaE16gBpbj218PcF5K+raFFKCQ7aKZ
AfjFB6X63iplcq8ySzQIedObQ61PGSFHwGUvesnhLervRDPLanJwS3Jfb0D9/pV1
2jftp1TDVx80y5UAaQW2/Y3glCoOGppSweSDXgC5pedJyb506GrVWrdQBvCZFGZ+
wP+mxEnaG5DXQoIizkzOVdKhTftCab3WFW9EpHG51QpKYeTh62P6bZuMNSASdNLq
03cF0HxLG2TeVdvVrKlzm1GmoY9JG/1CkLJx5uhY3137x0ZeuJ7arbeiHS7EiKwZ
```

Devemos guardar esta informação - chamada account-key - como ficheiro, para tal basta clicar no primeiro botão (que tem uma seta a apontar para um disco). A seguir ao download basta clicar em NEXT outravez.

3.2 VERIFICAÇÃO

A chave encontra-se agora registada e devemos ter à nossa frente uma janela parecida com esta:

1 Details
2 Verification
3 Certificate
NEXT

Verification

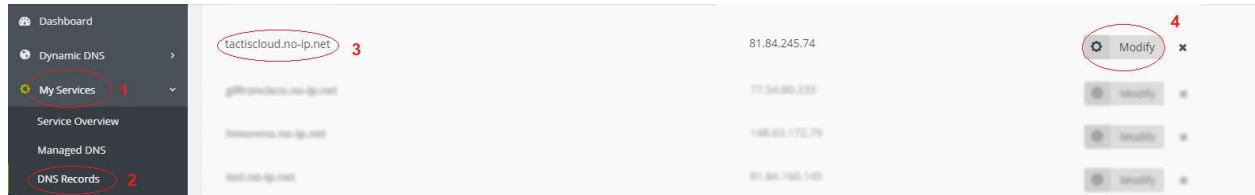
To verify domain ownership using DNS verification, you will need to create DNS records of TXT type as shown below. Please remember that it takes some time for new DNS records to become "visible", so you may need to wait for 15-20 minutes before clicking "Next". You can check whether your records became visible with the following command: "nslookup -q=TXT XXX", where XXX is one of the records as shown below.

Domain	TXT Record	Value
_acme-challenge.tactiscloud.no-ip.net		BC9QJ-Hq3q7N_BwKWqk6bwhR-B_qCnuRdEITnO25NWY

Devemos seguir as instruções mencionadas. Para isso vamos dirigir-nos a <https://www.noip.com/login> para adicionar o Domain TXT Record como requisitado, isto serve para provar que somos realmente os donos do domínio para o qual estamos a requisitar o certificado.

Depois de fazer-mos login devemos dirigir-nos a My Services > DNS Records > Selecionar o domínio pretendido (neste caso tactiscloud.no-ip.net) > Modify > Advanced Records > TXT.

Para melhor compreensão, podemos verificar as imagens abaixo:



1 –My Services, 2 –DNS Records, 3 – Encontrar o domain pretendido, 4 –Modify

Após seguir os ponto 1 a 4 devemos andar um pouco pra baixo na página até encontrarmos “Advanced Records” e aí devemos selecionar “TXT”

Advanced Records ⓘ



Agora devemos preencher um novo valor com os dados mencionados anteriormente:

Domain TXT Record	Value
_acme-challenge.tactiscloud.no-ip.net	BC9QJ-Hq3q7N_BwKWqk6bwhR-B_qCnuRdEITnO25NwY

Create Record

Hostname

☐ tactiscloud.no-ip.net
☒ _acme-challenge tactiscloud.no-ip.net
 Example: _acme-challenge.tactiscloud.no-ip.net

Data

BC9QJ-Hq3q7N_BwKWqk6bwhR-B_qCnuRdEITnO25NwY

Add

Para confirmar que o TXT Record foi adicionado com sucesso devemos abrir a linha de comandos e escrever:

`nslookup -q=TXT _acme-challenge.tactiscloud.no-ip.net`

Se o TXT record estiver corretamente adicionado os resultados serão:

```
Non-authoritative answer:
_acme-challenge.tactiscloud.no-ip.net text =
"BC9QJ-Hq3q7N_BwKWqk6bwhR-B_qCnuRdEITnO25NwY"
```

Após toda esta verificação podemos voltar ao <https://zerossl.com/free-ssl/#crt> que temos aberto e clicar em NEXT, se tudo correu conforme o previsto vamos ter o certificado pronto e mais dois ficheiros para fazer download, sendo eles o domain-crt e o domain-key respetivamente:



No final de todo este processo devemos ter connosco 4 ficheiros:

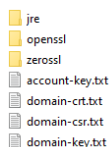
domain-csr.txt, account-key.txt, domain-crt.txt e domain-key.txt

3.3 CRIAR FICHEIROS

Para a criação do mesmo devemos copiar os ficheiros criados nos pontos 3.1 e 3.2 para uma pasta específica, neste exemplo essa pasta vai ser C:\tactis\certs

Também devemos copiar para essa pasta os ficheiros do ZeroSSL Portable Client, do OpenSSL e a pasta jre do Java, após isso devemos renomear as pastas para ficarem com nomes mais simples de entender.

Após estas cópias a pasta deve ter os seguintes conteúdos:



Todo este processo é feito por linha de comandos, por isso vamos abrir uma instância como administrador e dirigir-nos à pasta que acabamos de criar:

```
cd /D C:\tactis\certs
```

3.3.1 KEYSTORE.JKS

Para a utilização de conexões seguras por parte dos serviços é necessária a criação de um ficheiro keystore.jks.

Para criar esse ficheiro precisamos primeiro de criar um outro chamado pkcs.p12, que é criado da seguinte maneira:

```
openssl\openssl.exe pkcs12 -export -in domain-crt.txt -inkey domain-key.txt -out pkcs.p12 -name keybin
```

Após a criação do pkcs.p12 já podemos criar o keystore.jks:

```
jre\bin\keytool.exe -importkeystore -destkeystore keystore.jks -srckeystore pkcs.p12 -srcstoretype PKCS12 -alias keybin
```

Desta forma temos um keystore.jks que vai ficar válido durante 3 meses. Para o renovar podemos refazer todo o processo do ponto 3 ou seguir para o ponto 4 que vai explicar sobre a automatização da renovação de certificados.

3.3.2 CERTIFICADO .PFX

Para alguns outros serviços é necessário o uso de um ficheiro .PFX para ser acrescentado ao IIS do website.

Para gerar este ficheiro com base nas informações que já temos devemos fazer o seguinte:

```
openssl|openssl.exe pkcs12 -export -out tactiscloud.no-ip.net.pfx -inkey domain-key.txt -in domain-crt.txt
```

3.3.3 CRIAR CRT E KEY

Vamos agora criar um certificado e uma chave com base no certificado PFX que foi criado:

```
openssl|openssl.exe pkcs12 -in tactiscloud.no-ip.net.pfx -nocerts -out domain-crt.key
```

```
openssl|openssl.exe rsa -in domain-crt.key -out domain-crt.key
```

```
openssl|openssl.exe pkcs12 -in tactiscloud.no-ip.net.pfx -clcerts -nokeys -out domain-crt.crt
```

4. RENOVAR CERTIFICADOS

A renovação dos certificados pode ser feita através do ZeroSSL Client. Para que a automatização funcione, a mesma tem de ser feita no computador que disponibiliza o nosso domain em HTTP, neste caso esse computador é o PC-INFARMED, devemos ligar-nos por Ambiente de Trabalho Remoto, abrir uma linha de comandos como administrador e fazer o seguinte:

```
cd /D C:\inetpub\wwwroot
mkdir .well-known\acme-challenge
```

Agora devemos copiar a pasta em que estivemos a trabalhar (C:\tactis\certs\) para o PC-INFARMED e a partir dessa pasta correr o seguinte comando:

```
le64.exe --key account-key.txt --csr domain-csr.txt --csr-key domain-key.txt --crt domain-crt.txt --export-pfx
PASSWORDTACTIS --path C:\inetpub\wwwroot\.well-known\acme-challenge --unlink --issue-code 100 -live --
domains "tactiscloud.no-ip.net" --renew 90
```

Existem agora dois novos ficheiros, domain-crt.pfx e domain-crt.txt (foi substituído), que devemos usar para voltar a renovar o keystore.jks

4.1 COLOCAÇÃO E RENOVAÇÃO DOS FICHEIROS

Para que estes ficheiros que estivemos a criar possam ser usados têm que ser colocados nos seus devidos sítios.

Para renovar o ficheiro keystore.jks usado por um serviço específico basta aceder ao servidor e copiar o ficheiro para C:\NOMESVC\server\etc\

Para colocar um ficheiro PFX no IIS pela primeira vez é bastante simples, bastando aceder ao IIS, seleccionar Certificados de Servidor, Importar Certificado e escolher o certificado.

Para renovar um ficheiro PFX no IIS, se o processo for feito manualmente será simplesmente apagar o actual certificado e colocar o novo, no entanto é bom que isto seja feito de uma forma automática, essa forma não é tão simples para ser explicada neste manual, mas existe um ficheiro .bat que faz essa tarefa de uma forma automática.

Mais sobre os ficheiros .bat já existentes no ponto 5.

5. CONCLUSÃO

Com tudo isto, damos como concluído o manual de criação e renovação de certificados ZeroSSL.

Para todos os pontos falados já existe automatização criada e a funcionar para os certificados usados na Tactis, foram criados vários ficheiros em linguagem batch que são facilmente adicionados a uma tarefa programada do Windows que corre no primeiro dia de cada mês e renova e distribui todos os certificados pelas máquinas que o necessitam.

Estes batch files só funcionam na máquina a que estão agregados devido a menções de diversas pastas, no entanto os mesmo foram disponibilizados para análise na partilha em:

<\\192.168.70.70\partilha\CERTIFICADOS\batch>

Renovação JKS e PFX e distribuição: **renew_jks_pfx.bat**

O ficheiro acima não contém grandes comentários no código pois o mesmo já foi tocado neste manual.

Renovação de PFX no IIS: **renew_pfx_iis.bat**

O ficheiro acima contém bastantes comentários pois o processo não é simples de descrever.

Existem também batch files configurados em todos os computadores que têm serviços que usam o keystore.jks: **simple_copy.bat**

O intuito do ficheiro acima é substituir o keystore.jks dos serviços quando existir um novo.