

PKI

<https://linuxize.com/post/how-to-set-up-an-openvpn-server-on-centos-7/> Public Key Infraestructure

previa

orientado a la instalación de un **openvpn**

creación de los siguientes elementos:

- CA¹⁾
- SERVER certificate + key
- CLIENT certificate + key

usando la herramienta **easy-rsa**

CA

se recomienda crear todos estos ficheros en un servidor standalone / offline de la infraestructura que se monte

1. editar fichero **vars** (vars.example) para adecuar los valores (y hacer `source vars`)
2. `./easyrsa init-pki`
3. `./easyrsa build-ca` (opcionalmente, **nopass**)
 - genera los ficheros **ca.crt** y **ca.key**
 - con estos ficheros podremos firmar los *requests* de certificados para servidor y cliente

Deffie-Hellman

usado para el intercambio de llaves y firma HMAC, añadiendo una capa de seguridad adicional

1. `./easyrsa gen-dh`
 - el archivo **dh.pem** generado se copia en **/etc/openvpn/**
2. generar HMAC: `openvpn --genkey --secret ta.key`
 - el archivo **ta.key** generado se copia en **/etc/openvpn/**

servidor

1. `./easyrsa gen-req server1 nopass`
 - **server1** es el nombre que le asignamos
 - **nopass** para que no nos solicite la contraseña al arrancar (openvpn server)
 - genera **server1.key** (copiar en **/etc/openvpn/**) y **server1.req**
2. importar (en caso que la PKI la tengamos en otra máquina) la *requests* del servidor: `./easyrsa import-req server1.req server1`
 - **server1.req** es el fichero creado
 - **server1** nombre del servidor
 - este comando copia el fichero **server1.req** en **pki/reqs**
3. firmar la *request*: `./easyrsa sign-req server server1`
 1. el primer argumento puede ser **server** o **client**

2. el segundo argumento es el sh

1)

Certificate Authority

From:

<https://miguelangel.torresegea.es/wiki/> - **miguel angel torres egea**

Permanent link:

<https://miguelangel.torresegea.es/wiki/linux:certificados:pki?rev=1553251691>

Last update: **22/03/2019 03:48**

