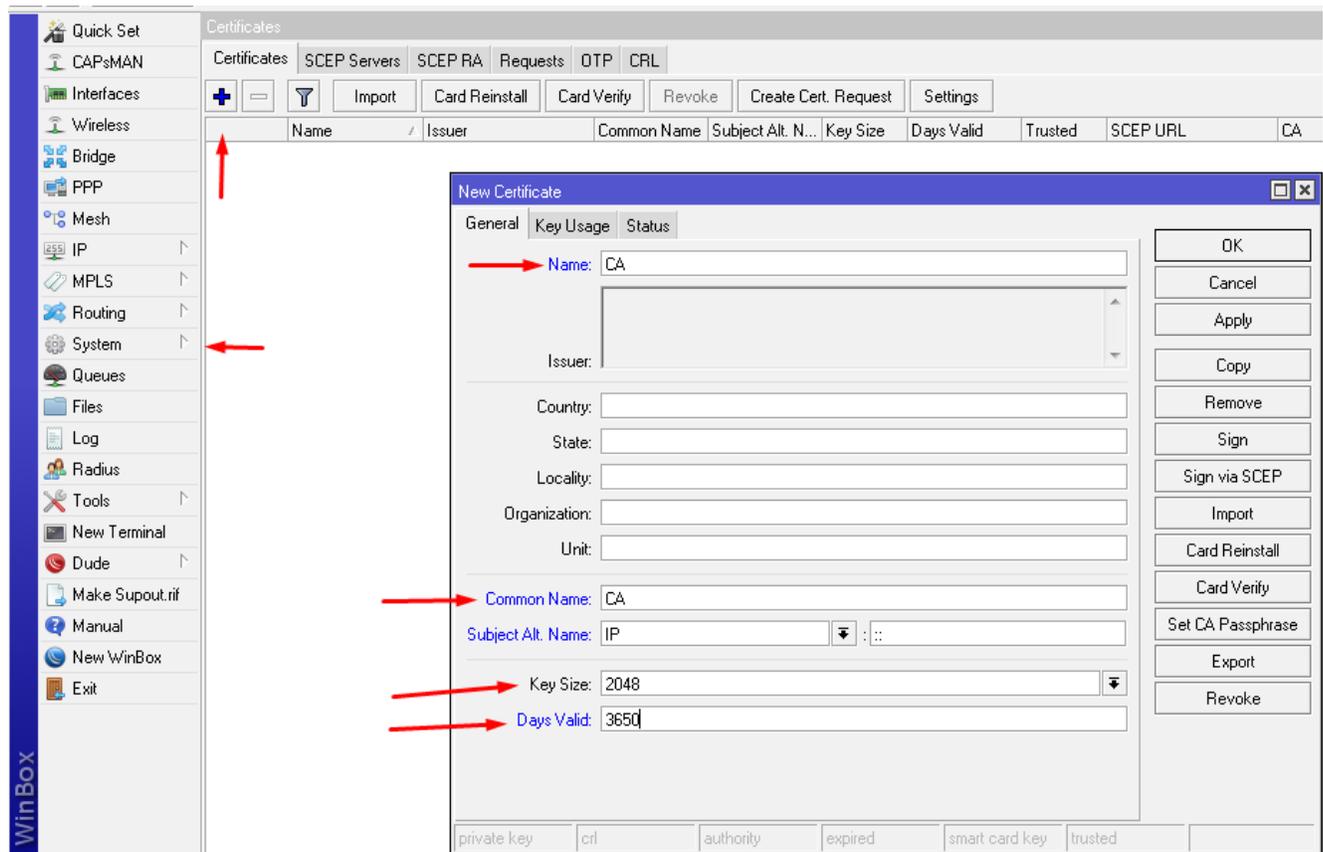


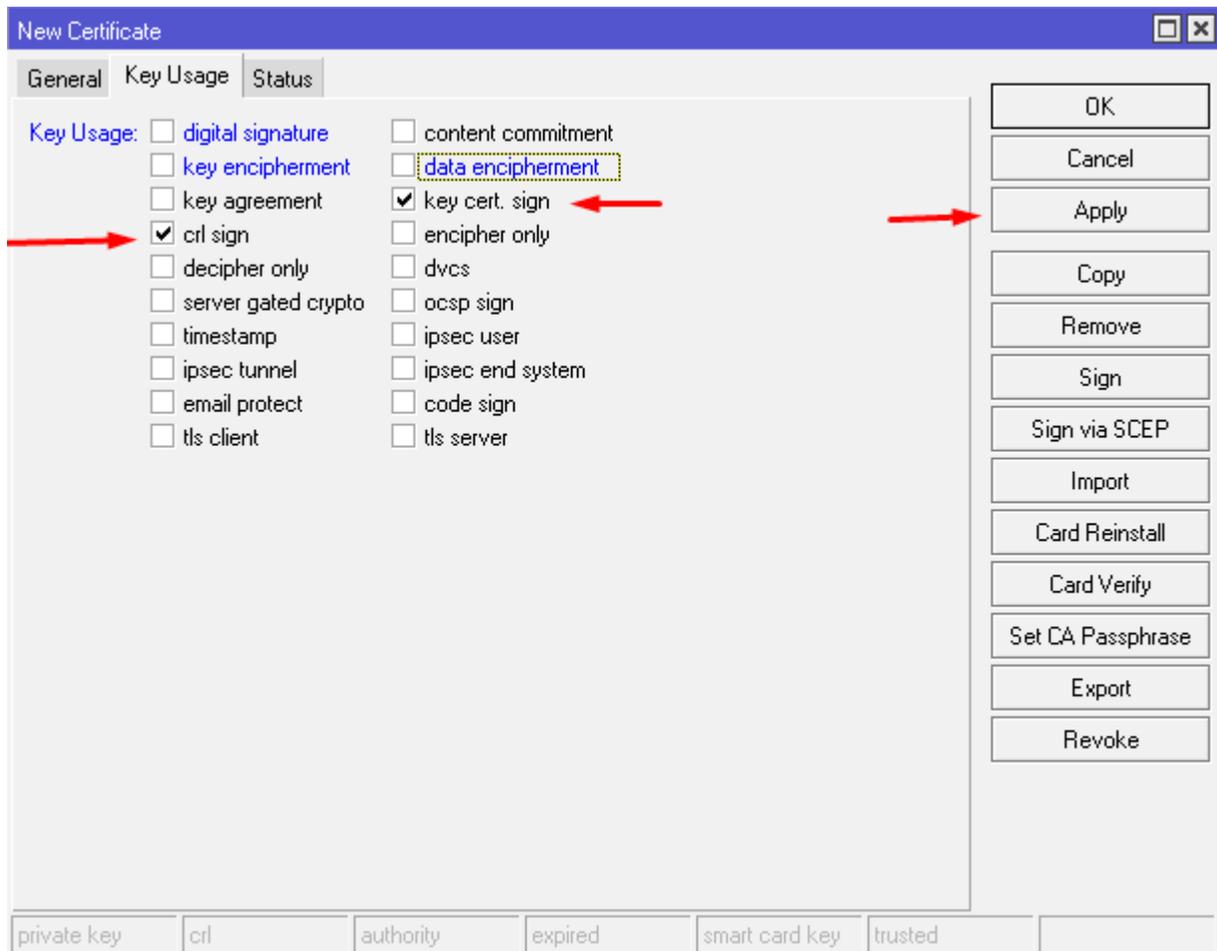
Laboratorio 1.1: Creación de certificados Públicos-privados Mikrotik.

Objetivos: Crear certificados digitales en su Router MikroTik.

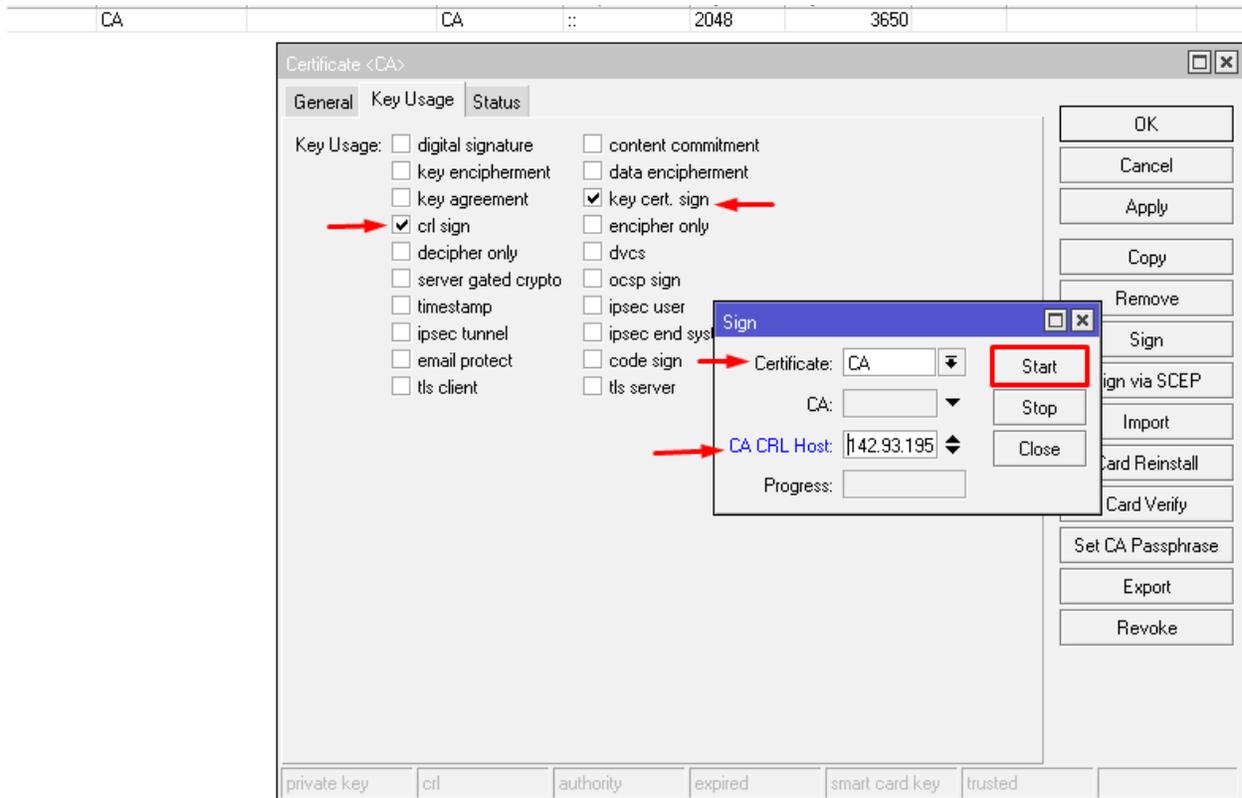
- **Paso 1:** en el primer paso nos dirigimos a **System** una vez allí damos click en certificados, luego damos click en **+** y procedemos a crear nuestro primer certificado Que será la Autoridad certificado (CA). En **Name:** ira el nombre, **Common Name:** repetir el nombre nuevamente, **Key Size:** nivel de encriptación del certificado crear, **Days Valid:** la cantidad de días que tendrá el certificado vigente.



- **Paso 2:** En este paso vamos definir los parámetros de nuestros certificados en donde seleccionaremos **CRL sing** y **Key Cert. Sing**, luego le damos a aplicar.



- **Paso 3:** Luego le damos a Sing para asignarle el host o el DDNS a nuestro certificado en **CA CRL Host**, luego damos Start.



Paso 4: Ahora vamos a crear nuestro certificado servidor Ojo los parámetros **Key Size** y **Days valid** serán los mismos que en el certificado anterior.

Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL	CA
KLAT	CA	CA	::	2048	3650	yes		CA

New Certificate

General | Key Usage | Status

Name: Server

Issuer:

Country:

State:

Locality:

Organization:

Unit:

Common Name: Server

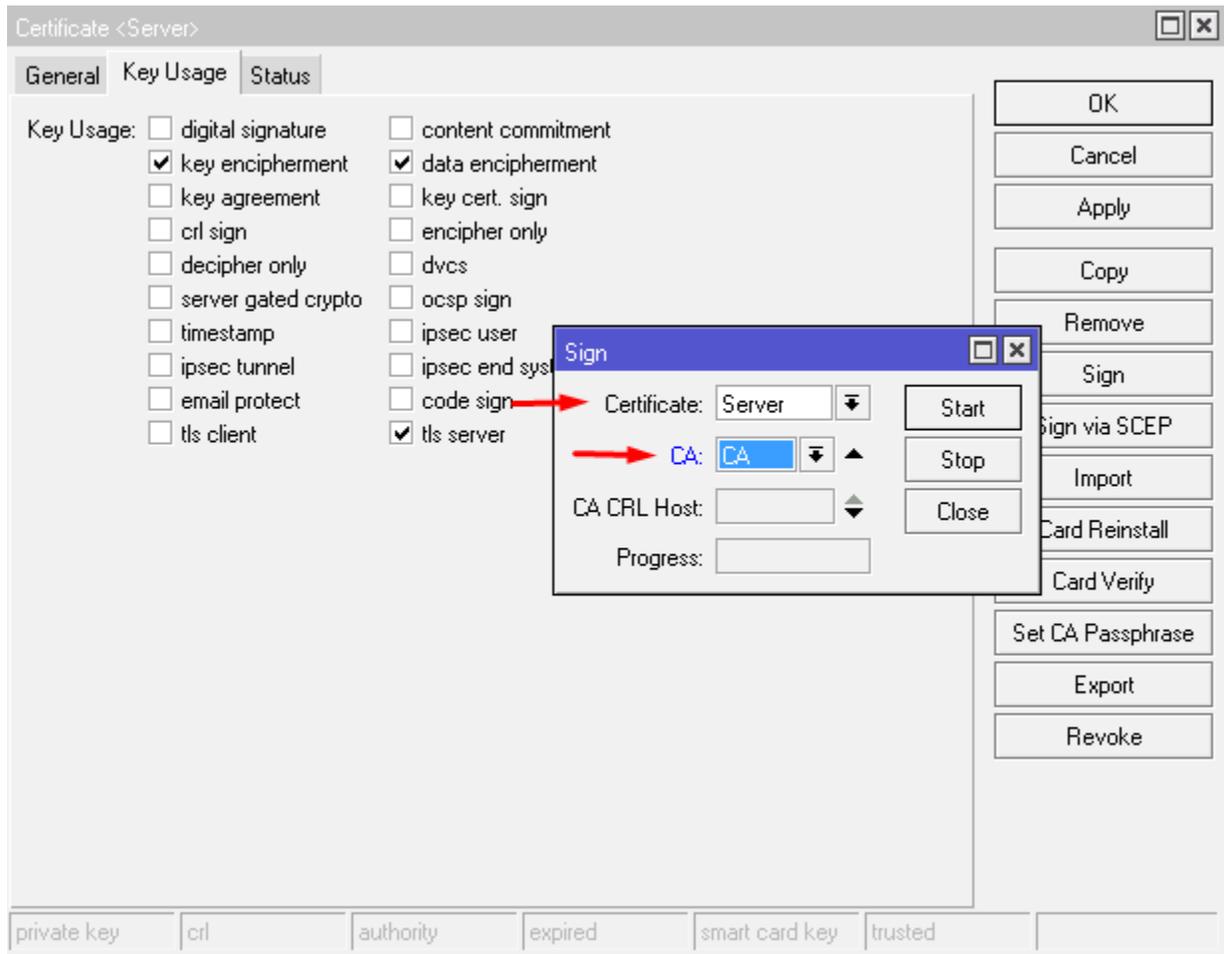
Subject Alt. Name: IP ::

Key Size: 2048

Days Valid: 3650

private key | crl | authority | expired | smart card key | trusted

Paso 6: En este paso vamos a sincronizar nuestro certificado servidor con el **CA** y luego le damos a **Start** .



Paso 7: Ahora vamos a crear el certificado cliente siguiendo los pasos del antiguo certificado a excepción de que en el **Key Usage** solo seleccionaremos **TLS Client**.

Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL	CA
KLAT	CA	CA	::	2048	3650	yes		CA
KI	Server			2048	3650	yes		CA

New Certificate

General | Key Usage | Status

Name: Cleinte

Issuer:

Country:

State:

Locality:

Organization:

Unit:

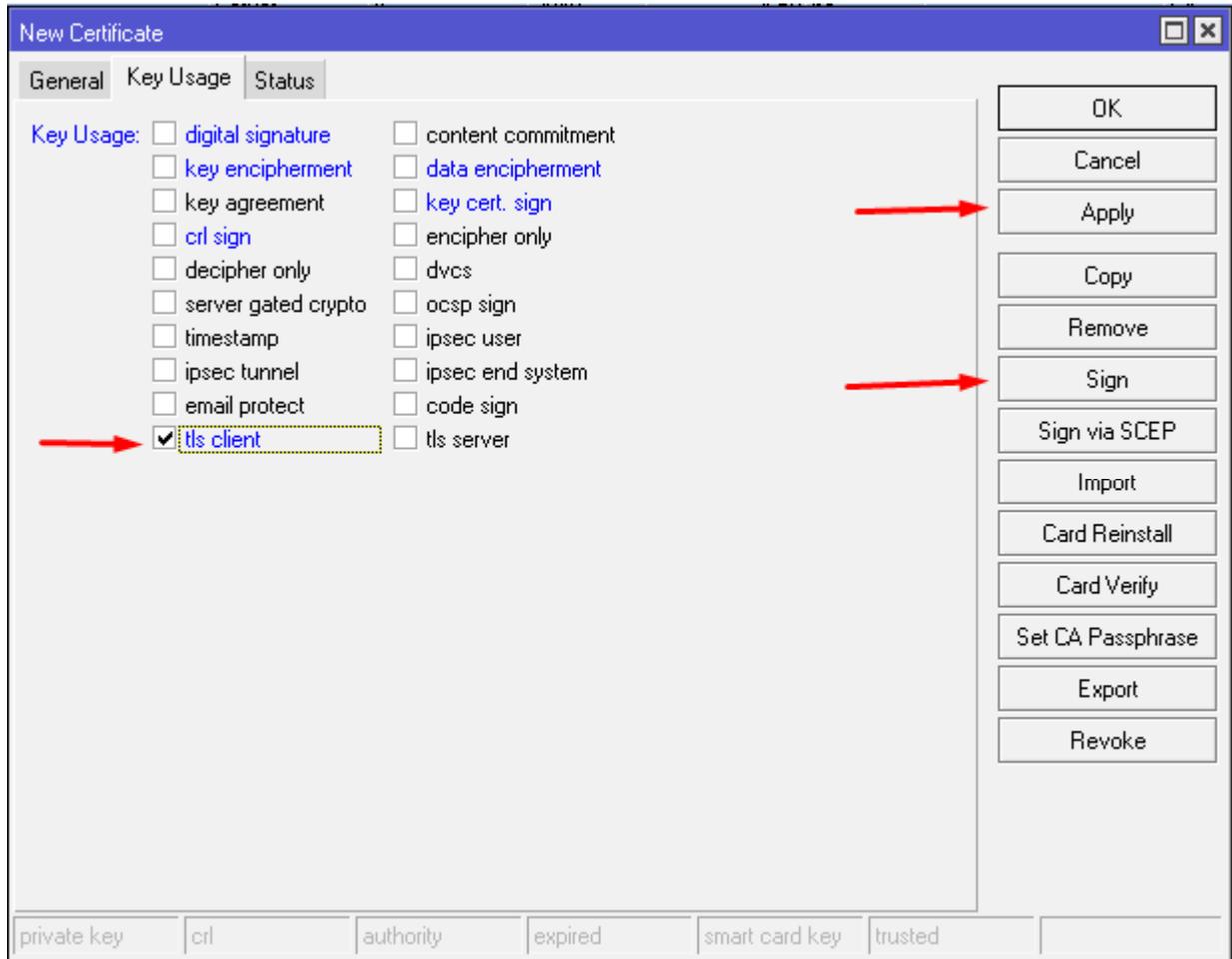
Common Name: Cleinte

Subject Alt. Name: IP ::

Key Size: 2048

Days Valid: 3650

private key | crl | authority | expired | smart card key | trusted



Paso 8: Ahora veremos nuestros certificados creados si todo se correctamente debe aparecerle como se muestra en la siguiente foto.

Certificates											
Certificates SCEP Servers SCEP RA Requests OTP CRL											
+ - [Filter] Import Card Reinstall Card Verify Revoke Create Cert. Request Settings											
	Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL	CA	Fingerprint	
KLAT	CA		CA	::	2048	3650	yes		CA	d633ebf2cdb...	
KI	Cliente		Cliente	::	2048	3650	no		CA	190c7131e7e...	
KI	Server		Server	::	2048	3650	no		CA	1b023eb744a...	