

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.

New Certificate				
General Key Usage Status	_			ОК
Key Usage: 📃 digital signature 🗌 key encipherment	content commitme	ent t		Cancel
key agreement	🖌 key cert. sign 🔫 🗌 encipher only			Apply
decipher only	dves oespisian			Сору
timestamp	ipsec user			Remove
ipsec tunnel	Ipsec end system			Sign
tls client	tls server			Sign via SCEP
				Import
				Card Reinstall
				Card Verify
				Set CA Passphrase
				Export
				Revoke
private key crl a	authority expired	d smart card key	trusted	



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

Certificate CA General Key Usage Status OK Key Usage: digital signature key encipherment data encipherment key agreement Key cert. sign V cri sign encipher only dvcs decipher only dvcs general progress progress: Statt ign via SCEP Import add Reinstall Progress: Card Verify Set CA Passphrase Export Revoke	CA		CA	::	2048	3650		
General Key Usage Status Key Usage: digital signature content commitment key encipherment data encipherment key agreement key cert. sign key digital signature content commitment key agreement key cert. sign encipher only dvcs copy copy server gated crypto cosp sign imestamp ipsec turnel ipsec turnel ipsec end system tts client Code sign CA CRL Host: [142:93.195 \$ Import Card Verify Stet CA Passphrase Export Revoke Revoke		Certificate <ca></ca>						
		General Key Us Key Usage:	sage Status digital signature key encipherment key agreement orl sign decipher only server gated crypto imestamp psec tunnel email protect its client	 content co data encipi key cert. si encipher oi dvcs ocsp sign ipsec user ipsec end sign code sign tils server 	mmitment herment gn ys Sign Certificate CA CRL Host Progress	: CA ₹ : 142.93.195 \$	Close	OK Cancel Apply Copy Remove Sign ign via SCEP Import ard Reinstall Card Verify Set CA Passphrase Export Revoke



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	∆ Iss	uer	Common Name	Subject Alt. N	Key Size	Days Valid	Trusted	SCEP UF	RL CA
KLAT	CA			CA	::	2048	3650	yes		
			New Certificate							
			General Key Usa	ge Status						01
				Server						
										Cancel
										Apply
			Issuer:						*	Сору
			Country:							Remove
			State:							Sign
			Locality:							Sign via SCEP
			Organization:							Import
			Unit:							Card Reinstall
		_		Server						Card Verify
			Subject Alt. Name:	IP		∓ :::				Set CA Passphrase
										Export
		_	Key Size:	2048						Revoke
		_	Days Valid:	3650						
			private key ci	·	authority	expired	smart card	key tru	usted	



Paso 5: En esta ocasión seleccionamos **Key encipherment y data encriphemerment,** luego le damos aplicar y luego Sing.

New Certificate						
General Key U	Isage Status					
Key Usage: 🗌	digital signature	content co	ommitment			ОК
	key encipherment	🗹 data encip	herment 🔫 🗕			Cancel
	key agreement	encipher o	ign Inlu			Apply
	decipher only		y			Сору
	server gated crypt timestamp	o ocspisign ipseciuser				Remove
	ipsec tunnel	ipsec end	system			Sign
	email protect tis client	Code sign ✓ tis server				Sign via SCEP
						Import
						Card Reinstall
						Card Verify
						Set CA Passphrase
						Export
						Revoke
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 .

Certificate <server></server>					
General Key Usage Status Key Usage: digital signature	 content co data encip key cert. si encipher o dvcs ocsp sign ipsec user ipsec end code sign ✓ tis server 	ommitment herment ign syst Sign Certificate CA CRL Hos Progress	e: Server ∓ A: CA ∓ ▲ t: 💽 ♀	Start Close	OK Cancel Apply Copy Remove Sign Sign via SCEP Import Card Reinstall Card Verify Set CA Passphrase Export Revoke
private key crl	authority	expired	smart card key	trusted	



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	Δ	Issuer	Common Name	Subject Alt. N	Key Size	Days Valid	Trusted	SCEP L	JRL	CA
KLAT	CA			CA	::	2048	3650	yes			
KI	Server		New Certificate								
	- † -		General Keullser	na Statue							
										OK	
			Name:	Cleinte						Cancel	
									× -		
										Apply	
			Issuer:						T	Сору	
			Country:							Remove	•
			State:							Sign	
			Locality:							Sign via S(ΈP
			Organization:							Import	
			Unit:							Card Rein:	stall
		_	Common Name:	Cleine						Card Veri	ífy
			Subject Alt, Name:	IP		Ŧ :::				Set CA Passp	ohrase
				00.40						Export	
			Key Size:	2048						Revoka	
			Days Valid:	3650							
			private key crl	1	authority	expired	smart card	key tri	usted		



New Certificate					
New Certificate General Key Usage Stal Key Usage: digital signa key enciph key agreen crl sign decipher or server gate timestamp ipsec tunne email prote	tus ature erment data enci erment data enci encipher encipher d crypto d cr	ommitment pherment sign only r I system			OK Cancel Apply Copy Remove Sign Sign via SCEP Import Card Reinstall Card Verify Set CA Passphrase Export Revoke
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 0	TP CRL							
+ -	T Import	Card Reinstall Card	Verify Revok	e Create Cer	rt. Request	Settings				
	Name 🛛 🕹	Issuer	Common Name	Subject Alt. N	Key Size	Days Valid	Trusted	SCEP URL	CA	Fingerprint
KLAT	CA		CA	::	2048	3650	yes			d633ebf2cdb
KI	Cliente		Cliente	::	2048	3650	no		CA	190c7131e7e
KI	Server		Server	::	2048	3650	no		CA	1b023eb744a