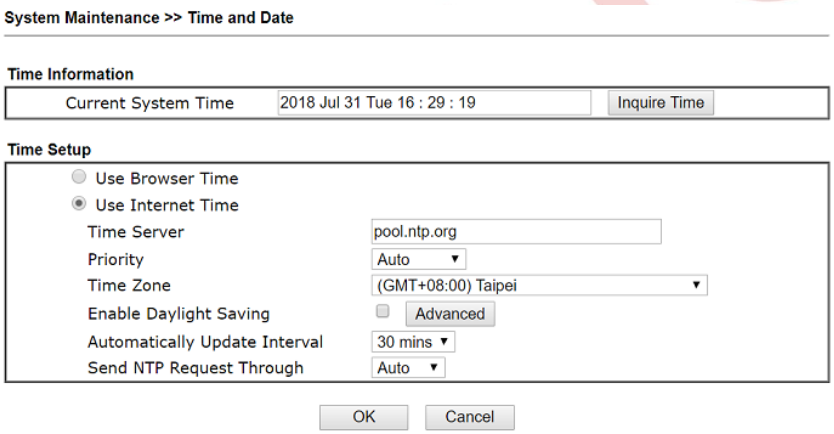
VIGOR ROUTER'DA XCA İLE OpenVPN KURUUMU

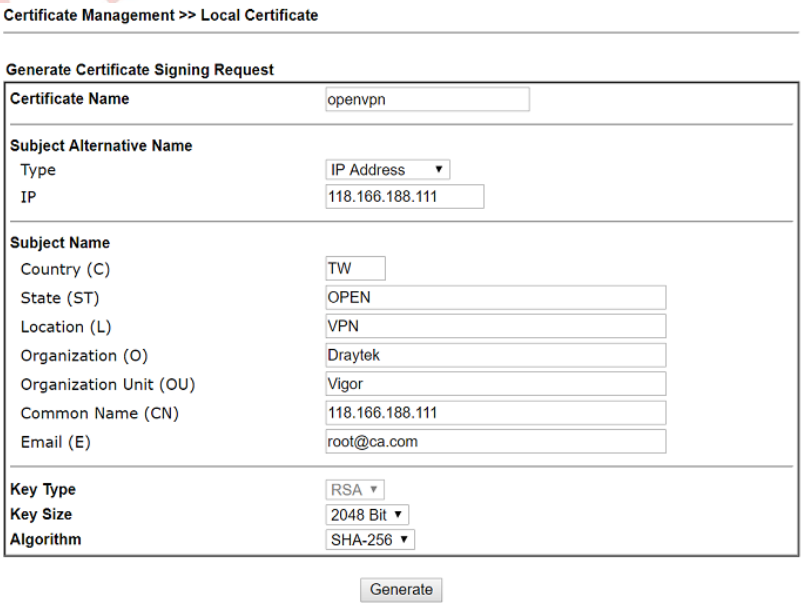
OpenVPN, ağ santralleri için SSL/TLS kullanan özel bir güvenlik protokolü kullandığından network address translators (NAT) ve Firewall'a geçiş yapabilen açık kaynaklı bir VPN teknikleridir. Sertifika OpenVPN'in desteklediği client kimlik doğrulama yöntemlerinden biridir. Sertifikayı imzalamak için bir Certificate Authority (CA) yazılımı olan XCA'yı kullanacağız. Bu makale şunları içermektedir.

Bölüm 1. Router Üzerinde Server Sertifikası Yapma

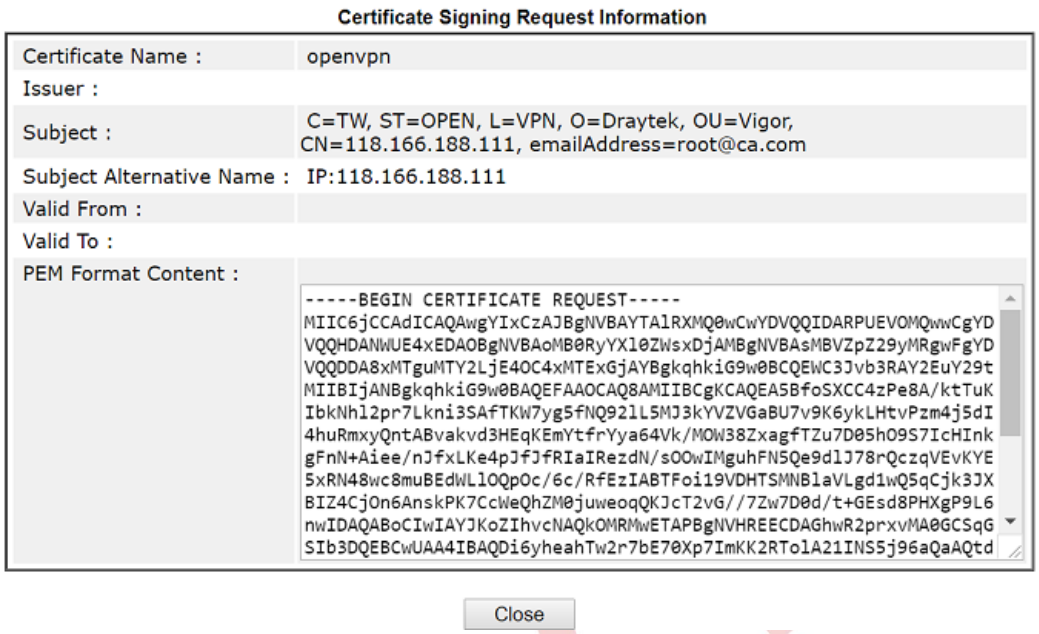
1-1. Sertifikanın geçerli bir süresi olduğundan routerın saat ayarlarının **System Maintenance >> Time and Date** sayfasından doğru olup olmadığını kontrol edin.



1-2. Yeni bir sertifika oluşturmak için **Certificate Management >> Local Certificate** sayfasına gidin. Bilgileri doldurun ve sonra **Generate'**e tıklayın.

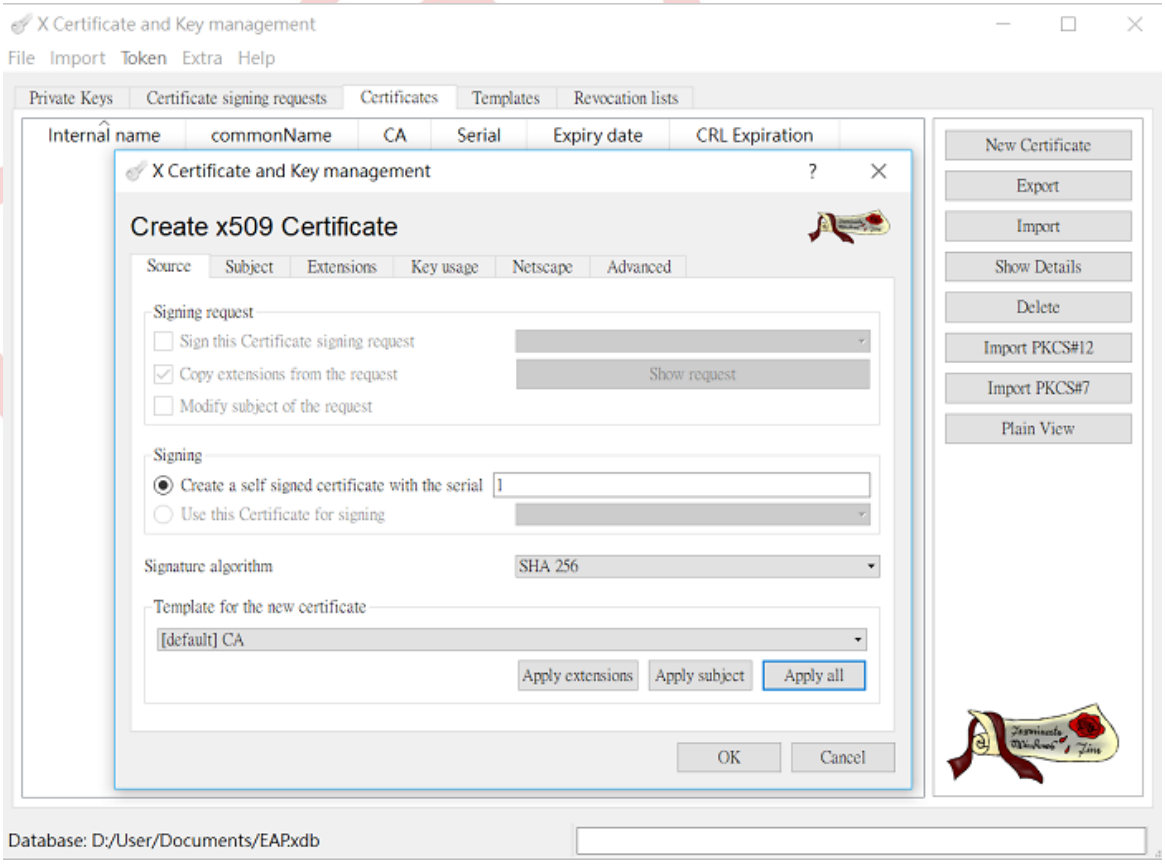


1-3. Generate'e tıkladıktan sonra CA tarafından imzalanması gereken Sertifika Sign Request 'i göreceksiniz. Sertifikayı PEM Format Content'den kopyalayın.



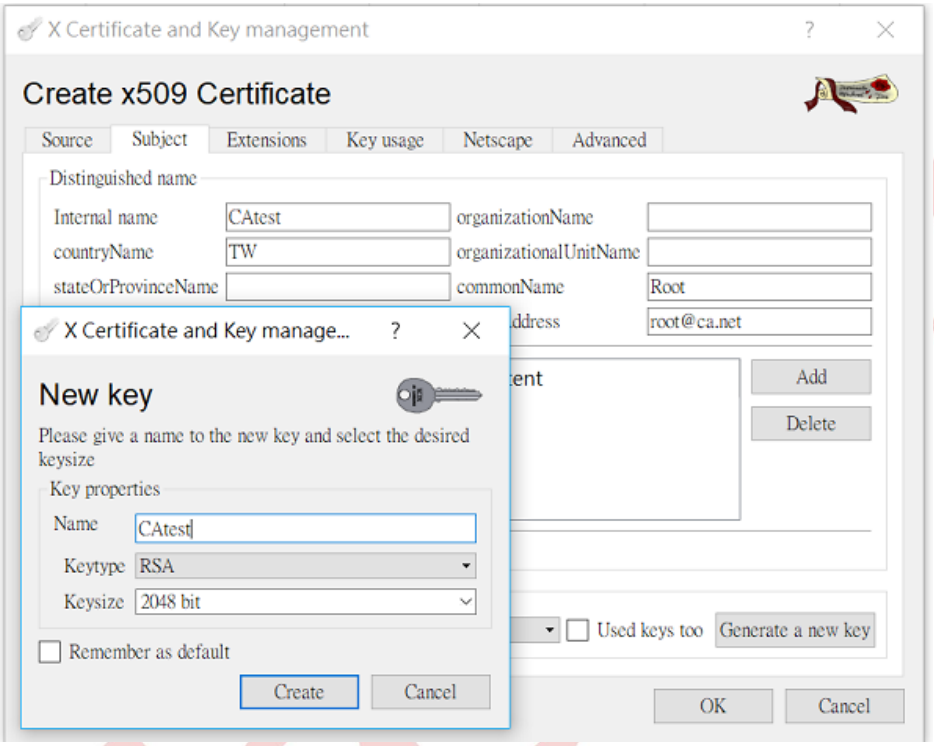
Bölüm 2. XCA'da Yeni Bir CA Oluşturma

2-1. XCA'yı başlatın Certificates sekmesine gidin **New Certicate**'e tıklayın. **Create a self-signed Certificate with the serial**'i seçin. CA şablonunu uygulamak için **Apply all**'a tıklayın.



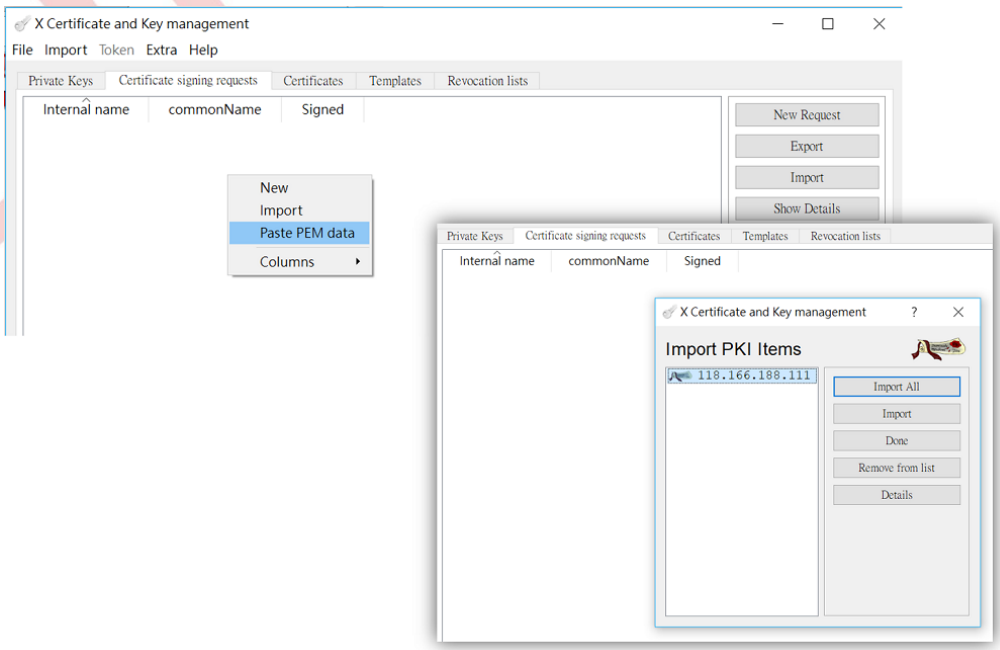
2-2. Subject sekmesine gidin.

- Sertifika için ayırt edici özellikler girin sonra **Generate a new key**'e tıklayın.
- **Keytype** için "RSA" ve **Keysize** için "2048 bit" seçin sonra **Create**'e tıklayın.
- CA sertifikasını oluşturmak için OK'a tıklayın. Artık server sertifikası ve client sertifikası imzalamak için Trusted (Güvenilir) CA Sertifikamız var.

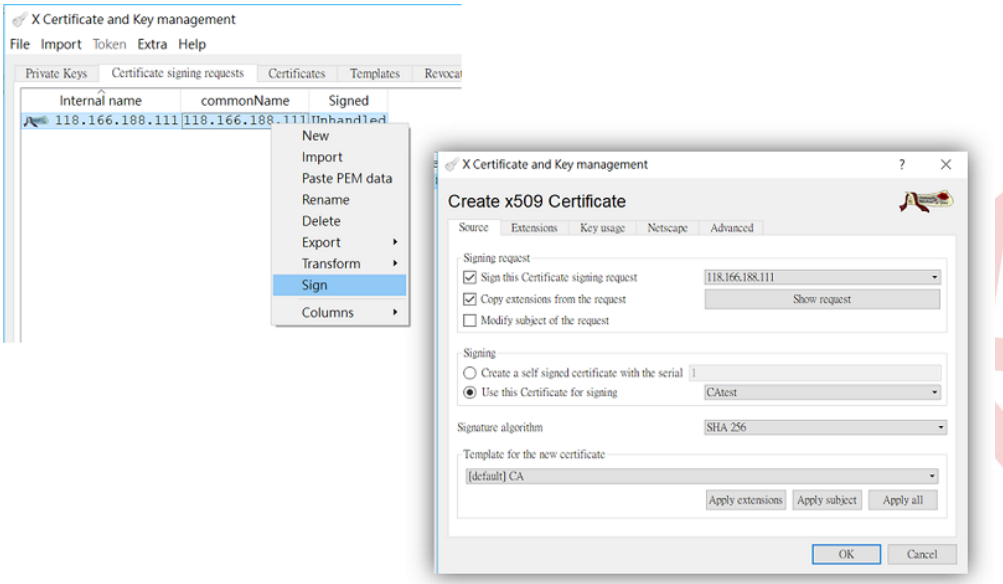


Bölüm 3. Signed Server Certificate ve CA Certificate Router'a Alma

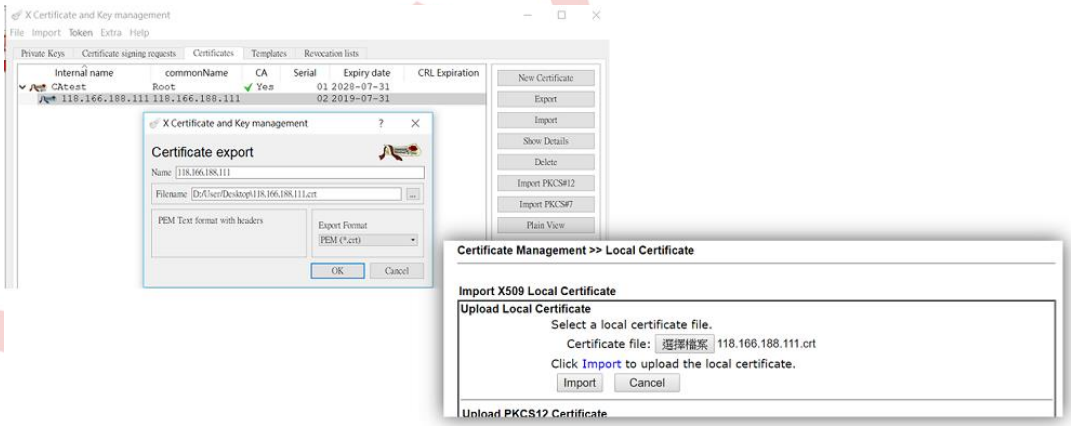
3-1. Certificate signing requests sekmesine gidin. Paste PEM data'yı seçin ve 1-3'te routerdan kopyalanan PEM Format Content'ini yapştırın.



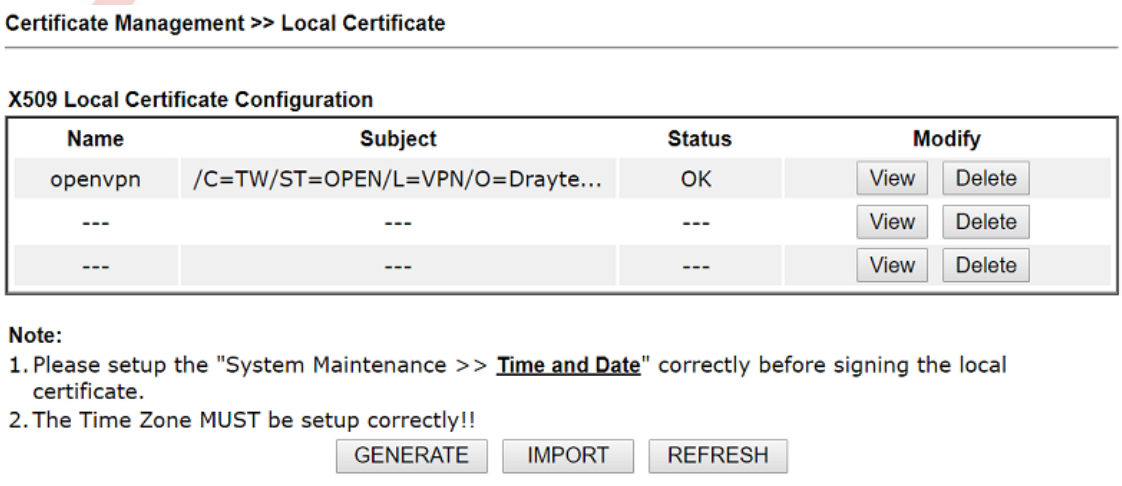
3-2. Alınan sertifikayı sağ tıklayın ve **Sign** seçeneğini seçin. İmzalamak 2. adımda oluşturulan sertifikayı kullanın.



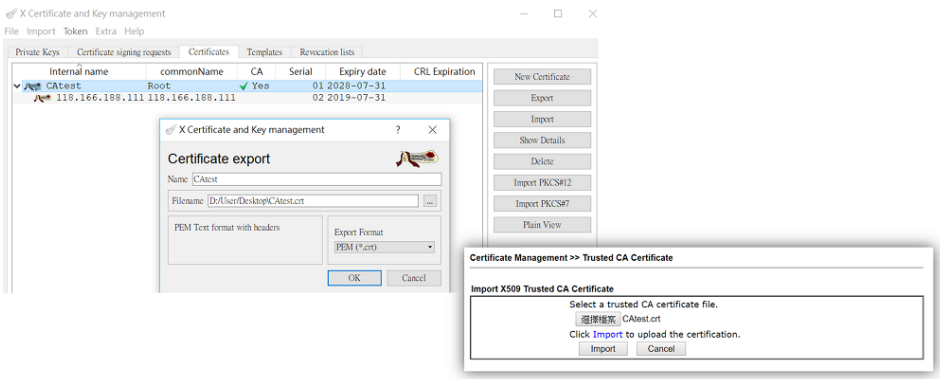
3-3. Signed Local Certificate'i .crt formatında export edin. Router'ın GUI'sine geri dönün ve expport edilen belgeyi **Certificate Management >> Local Certificate >> Upload Local Certificate** sayfasından routera alın.



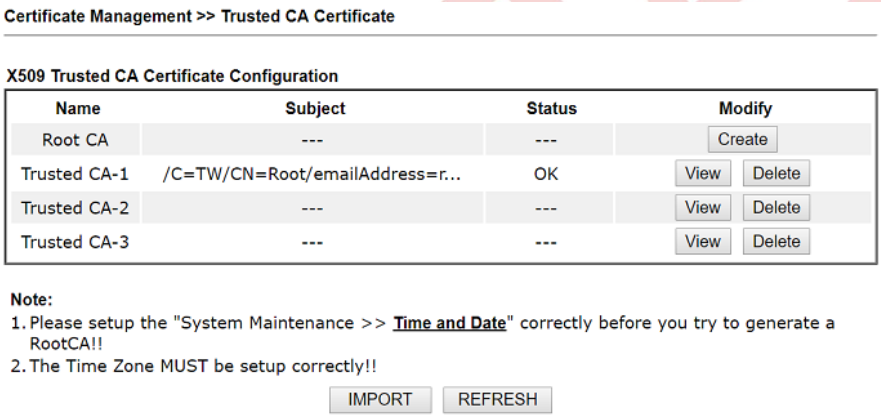
3-4. Yüklenen sertifikanın durumunun OK olduğundan emin olun.



3-5. XCA'da Certificate sekmesine gidin CA sertifikasını seçin ve .crt formatında dışarı aktarın. **Certificate Management >> Trusted CA Certificate** sayfasından routera alın.



3-6. Alınan Trusted CA'nın durumunun **OK** olduğundan emin olun.



Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

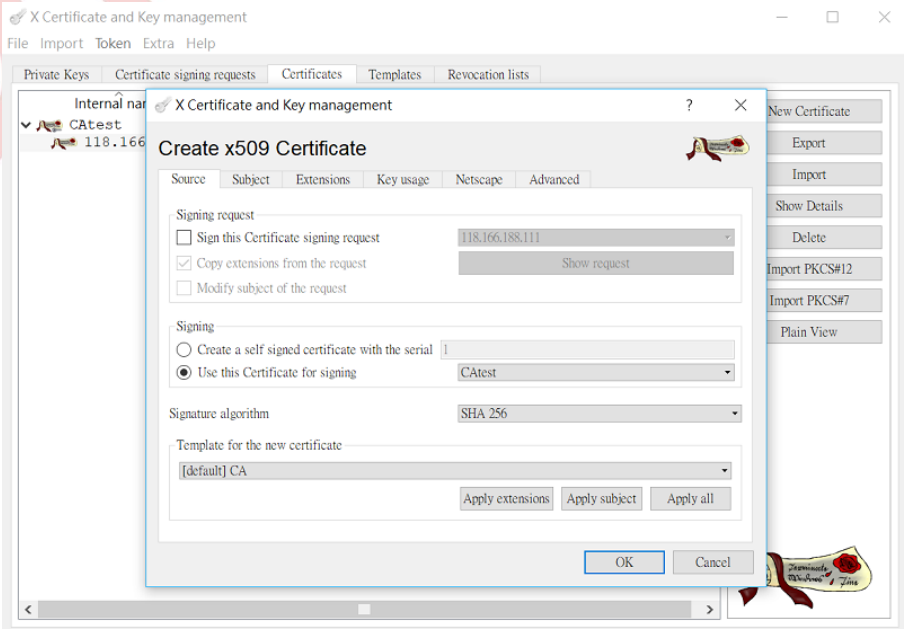
Name	Subject	Status	Modify
Root CA	---	---	Create
Trusted CA-1	/C=TW/CN=Root/emailAddress=r...	OK	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

Note:
1. Please setup the "System Maintenance >> **Time and Date**" correctly before you try to generate a RootCA!!
2. The Time Zone MUST be setup correctly!!

IMPORT REFRESH

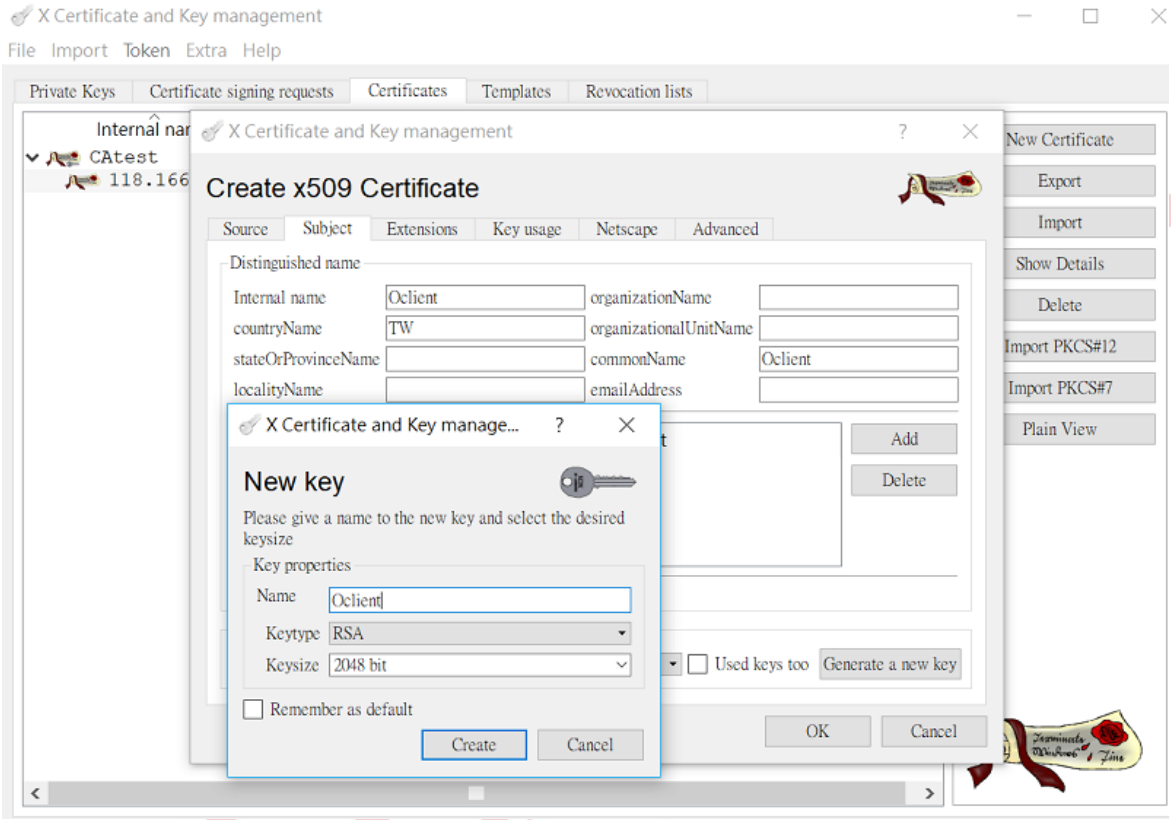
Bölüm 4. VPN Client için Private Sertifika ve Private Key Oluşturma

4-1. XCA'da Certificates'e gidin, **New Certificate**'e tıklayın. Signing başlığı altında imzalanan sertifikayı kullanmak için Use this Certificate for signing 2i seçin.

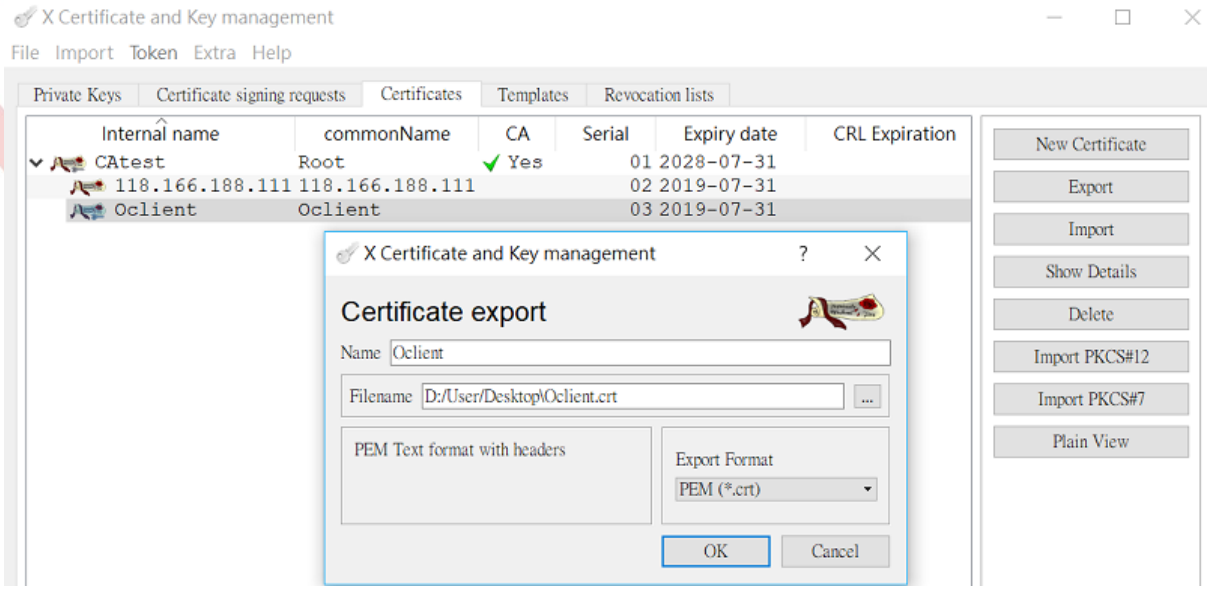


4-2. Subject sayfasına gidin.

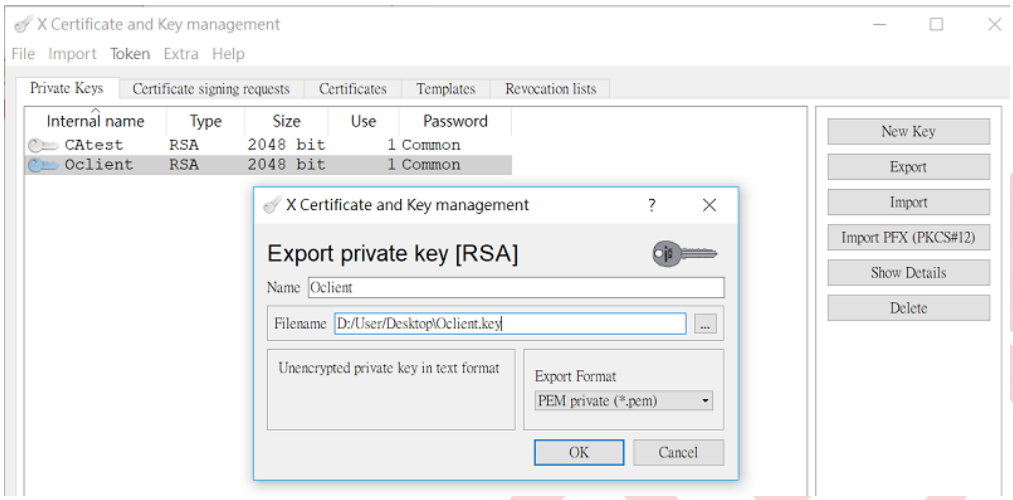
- Sertifika için ayırt edici özellikler girin sonra **Generate a new key**'e tıklayın.
- **Keytype** için "RSA" ve **Keysize** için "2048 bit" seçin sonra **Create**'e tıklayın.
- CA sertifikasını oluşturmak için OK'a tıklayın. Artık VPN Client'ı içinde özel bir sertifikamız var.



4-3. Certificates'e gidin, yeni oluşturduğunuz sertifikayı seçin. Sertifikayı .crt formatında dışa aktarın ve VPN Client'ına ekleyin.

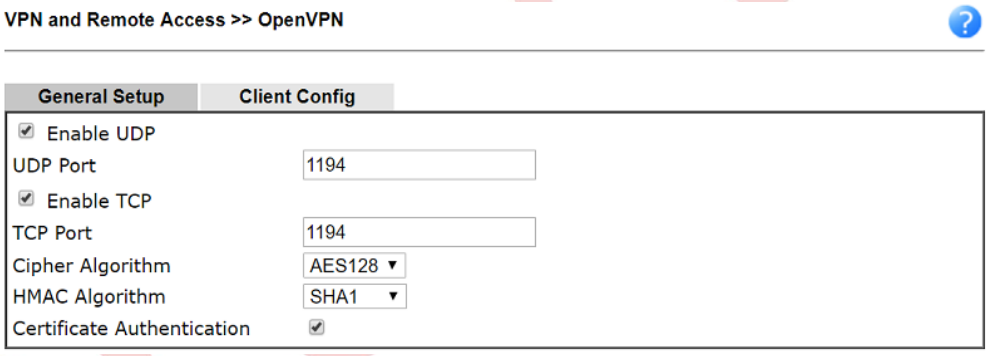


4-4. Private Keys'e gidin, Private Key (Oclien.key) dışa aktarın, uzantı adını elle .key olarak değiştirin. Ardından VPN Client'a ekleyin.

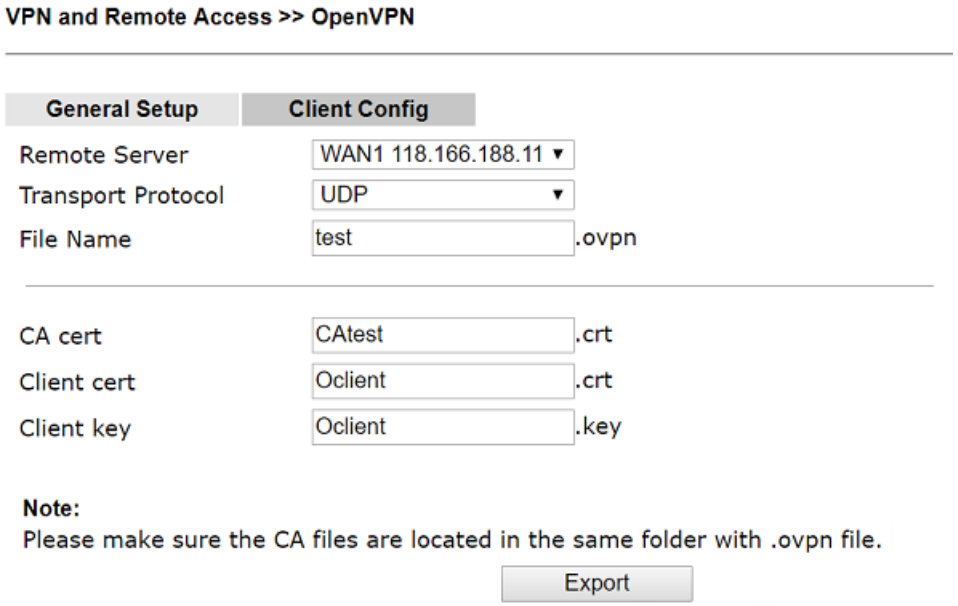


Bölüm 5. OpenVPN Serveri olarak Router Kurulumu

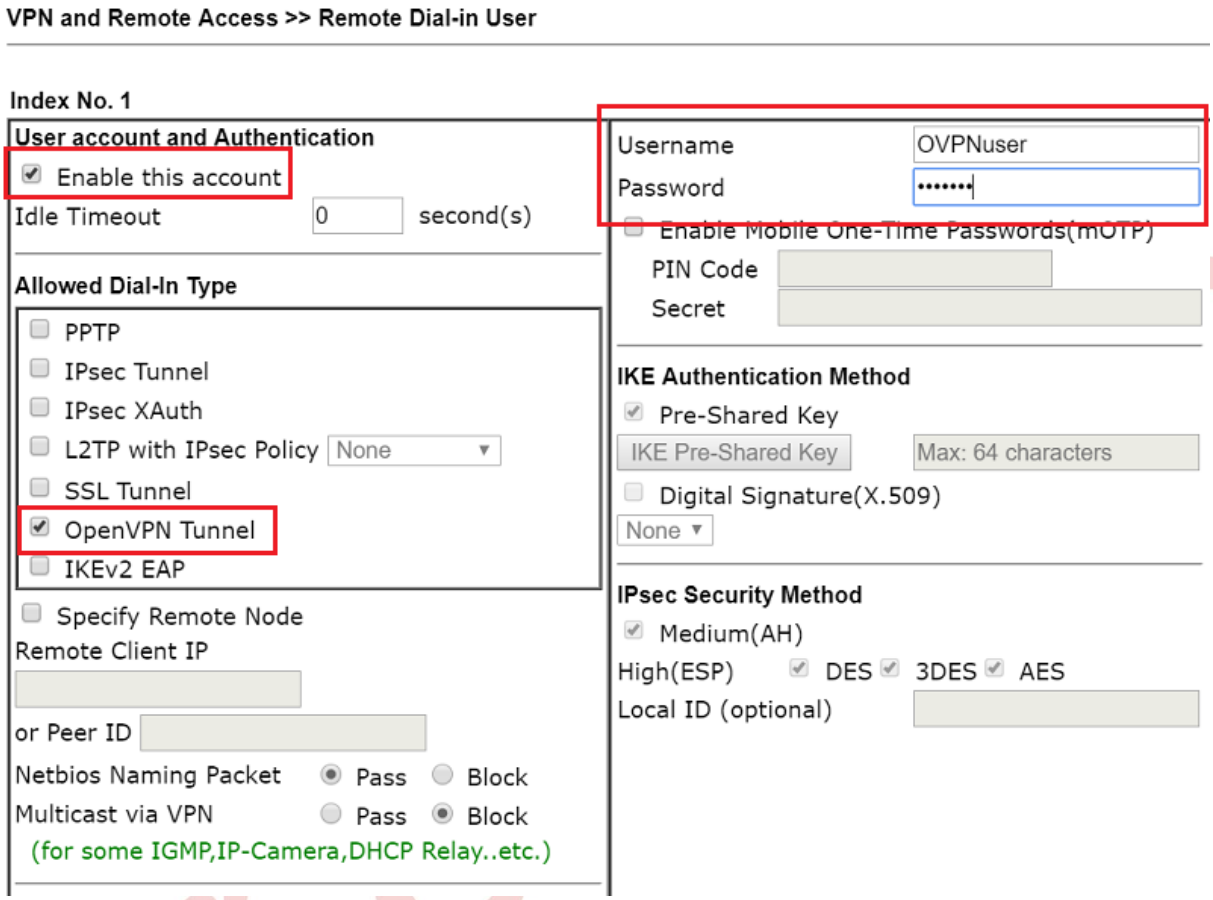
5-1. **VPN and Remote Access >> OpenVPN General Setup** sayfasına gidin ve görseldeki konfigürasyonları yapın.



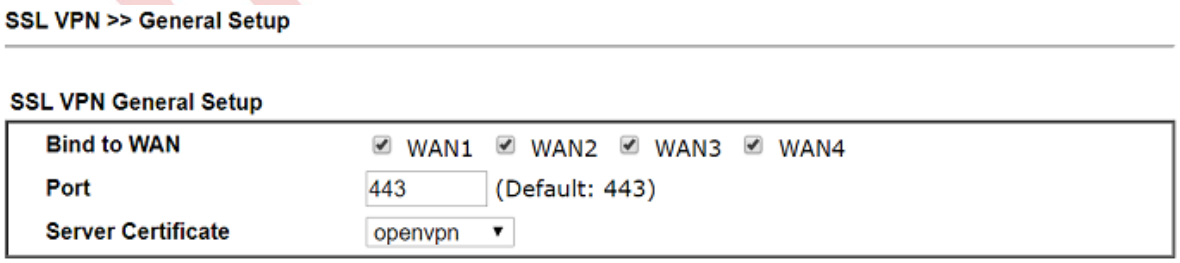
5-2. Client Config sekmesine gidin. CA Certificate, Client Certificate ve Client Key dosya adlarını belirtin. Sonra **Export**'a tıklayın.



5-3. OpenVPN Dial-in kullanıcılarına yeni kullanıcı profili oluşturmak için **VPN and Remote Access >> Remote Dial-in User** sayfasına gidin. **Enable this account**'u etkinleştirin. **Username/Password** girin ve Allowed Dial-in Type'de **OpenVPN Tunnel**'i etkinleştirin.



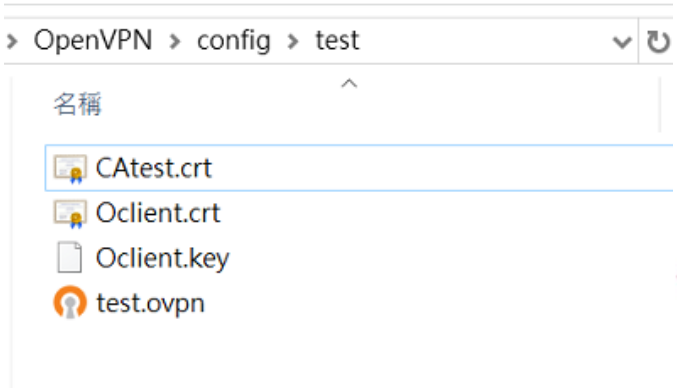
5-4. Server sertifikasını bölüm 2'de oluşturulan Local sertifikaya değiştirmek için **SSL VPN >> General Setup** sayfasına gidin.



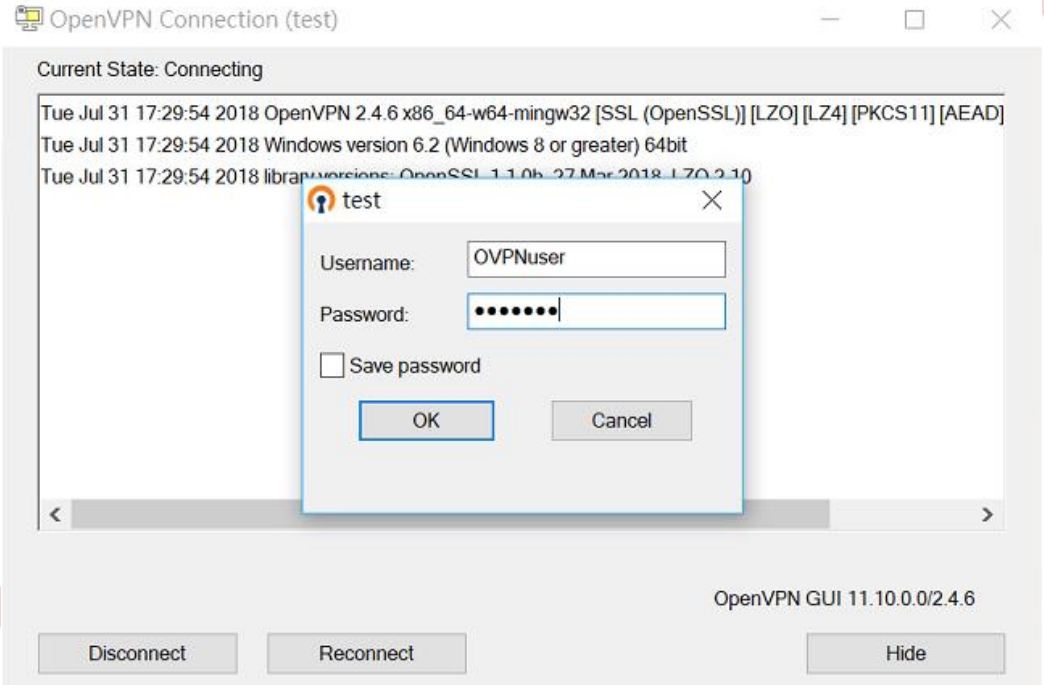
Bölüm 6. OpenVPN GUI'de Client Kurulumu

6-1. OpenVPN konfigürasyonunu (test.vpn) OpenVPN GUI'ye aktarın. OpenVPN config klasörüne koymak için üç dosya vardır.

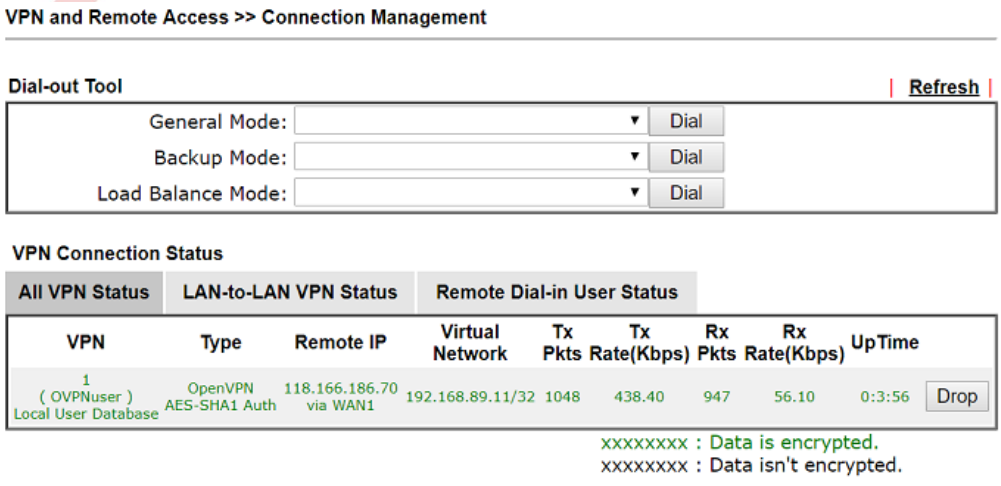
- Trusted CA Certificate (CAtest.crt)
- Private Certificate (Oclient.crt)
- Private Key (Oclient.key)



6-2. **Connect**'e tıklayın ve 5-3 adımdaki yapılandırılan username/password girin.



OpenVPN Tunnel'i kurulduktan sonra VPN durumunu **VPN and Remote Access >> Connection Management** sayfasından görebilirsiniz.



Sorun Giderme

VERIFY ERROR: error=self signed certificate

Router içe aktardığımız sertifika yerine VPN için kendinden imzalı sertifika kullanıyor. SSLVPN >> General Setup sayfasında Server Sertifikası ayarlarını kontrol edin (adım 5-4).