



## Generating a Certificate Signing Request (CSR) using Cisco IOS VPN router

### ***Private key and CSR for Cisco IOS VPN router***

In this section, we describe how to build a CSR (Certificate Signing Request) as well as a private key for the Cisco IOS VPN router.

Building the CSR for the router :

```
# cd /local/openssl
# openssl req -config /local/openssl/conf/openssl.cnf -new -out
CA/vpn-server-req.pem -keyout CA/private/vpn-server-key.pem -
days 365
```

Note : do not forget the passphrase for the generated private key.

The actual request that will be processed by the CA is stored in the *vpn-server-req.pem* file. The CN for the request has been set to VPN-SERVER.

### ***Private key and CSR for the VPN clients***

A particular attention must be given to the CSR for the clients, as the OU field in the DN must match the group parameter in the router's configuration.

We chose 'INTRANET-ACCESS' as both the OU field in the DN of the CSR and the group parameter in the router's configuration.

Note : depending on the router's configuration, the group parameter 'INTRANET-ACCESS' can be stored in the router's configuration or in a RADIUS/TACACS external database. We show an example of a router's configuration that allows for a RADIUS storage of the group parameter further in this document.

Building the CSR for the INTRANET-ACCESS group

```
# cd /local/openssl
# openssl req -config /local/openssl/conf/openssl.cnf -new -out
CA/client-intranet-access-req.pem -keyout CA/private/client-
intranet-access-key.pem -days 365
```

Note : do not forget the passphrase for the generated private key.

The actual request that will be processed by the CA is stored in the *client-intranet-access-req.pem* file. The CN for the request has been set to 'CLIENT-INTRANET-ACCESS'.