#
# OpenSSL example configuration file.
# This is mostly being used for generation of certificate requests.
#
RANDFILE = /dev/arandom
[ca]
default\_ca = CA\_default
[CA\_default]
dir = /etc/openvpn
certificate = $dir/xx.crt
private\_key = $dir/xx.key
serial = $dir/serial
database = $dir/index.txt
new\_certs\_dir = $dir/
default\_md = md5
policy = policy\_match
default\_days = 3500
[policy\_match]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
#######################################
[ req ]
default\_bits = 1024
default\_keyfile = privkey.pem
distinguished\_name = req\_distinguished\_name
attributes = req\_attributes
[ req\_distinguished\_name ]
countryName = Country Name (2 letter code)
#countryName\_default = AU
countryName\_min = 2
countryName\_max = 2
stateOrProvinceName = State or Province Name (full name)
#stateOrProvinceName\_default = Some-State
localityName = Locality Name (eg, city)
0.organizationName = Organization Name (eg, company)
#0.organizationName\_default = Internet Widgits Pty Ltd
# we can do this but it is not needed normally :-)
#1.organizationName = Second Organization Name (eg, company)
#1.organizationName\_default = CryptSoft Pty Ltd
organizationalUnitName = Organizational Unit Name (eg, section)
#organizationalUnitName\_default =
commonName = Common Name (eg, fully qualified host name)
commonName\_max = 64
emailAddress = Email Address
emailAddress\_max = 64
[ req\_attributes ]
challengePassword = A challenge password
challengePassword\_min = 4
challengePassword\_max = 20
unstructuredName = An optional company name
[ x509v3\_extensions ]
nsCaRevocationUrl = http://www.cryptsoft.com/ca-crl.pem
nsComment = "This is a comment"
# under ASN.1, the 0 bit would be encoded as 80
nsCertType = 0x40
#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName
#nsCertSequence
#nsCertExt
#nsDataType