

```
1 HOME = .
2 RANDFILE = $ENV::HOME/.rnd
3 oid_section = new_oids
4
5 [ new_oids ]
6
7 [ ca ]
8 default_ca = openvpn
9
10 [ openvpn ]
11 dir = /etc/openvpn/ca/
12 certs = $dir
13 crl_dir = $dir
14 database = $dir/index.txt
15 new_certs_dir = $dir
16 certificate = $dir/cacert.pem
17 serial = $dir/serial
18 crl = $dir/crl.pem
19 private_key = $dir/cakey.pem
20 RANDFILE = $dir/.rand
21 x509_extensions = usr_cert
22 default_days = 999999
23 default_crl_days= 30
24 default_md = sha256
25 preserve = no
26 policy = policy_match
27 email_in_dn = no
28 extendedKeyUsage= serverAuth
29 keyUsage = digitalSignature, keyEncipherment
30
31 [ policy_match ]
32 countryName = optional
33 stateOrProvinceName = optional
34 organizationName = optional
35 organizationalUnitName = optional
36 commonName = supplied
37 emailAddress = optional
38
39 [ req ]
40 default_bits = 2048
41 default_keyfile = privkey.pem
42 distinguished_name = req_distinguished_name
43 attributes = req_attributes
44 x509_extensions = v3_ca
45 string_mask = nombstr
46 x509_extensions = usr_cert
47
48 [ req_distinguished_name ]
49 countryName = Country Name (2 letter code)
50 countryName_default = DE
51 countryName_min = 2
52 countryName_max = 2
53
54 stateOrProvinceName = State or Province Name (full name)
55 stateOrProvinceName_default = Niedersachsen
56
57 localityName = Locality Name (eg, city)
58 #localityName_default = Loxstedt
59
60 0.organizationName = Organization Name (eg, company)
61 0.organizationName_default = blablaName
62
63 organizationalUnitName = Organizational Unit Name (eg, section)
64 #organizationalUnitName_default =
65
66 commonName = Common Name (eg, your name or your server\'s hostname)
67 commonName_max = 64
68
69 emailAddress = Email Address
```

```
70 emailAddress_max      = 40
71
72 [ req_attributes ]
73 challengePassword     = A challenge password
74 challengePassword_min = 4
75 challengePassword_max = 20
76 unstructuredName     = An optional company name
77
78 [ usr_cert ]
79 basicConstraints=CA:FALSE
80 nsComment        = "OpenSSL Generated Certificate"
81 subjectKeyIdentifier      = hash
82 authorityKeyIdentifier    = keyid,issuer:always
83 keyUsage             = nonRepudiation, digitalSignature, keyEncipherment
84 extendedKeyUsage      = serverAuth, clientAuth, codeSigning, emailProtection
85
86 [ v3_req ]
87 basicConstraints = CA:FALSE
88 keyUsage         = nonRepudiation, digitalSignature, keyEncipherment
89 extendedKeyUsage = serverAuth, clientAuth, codeSigning, emailProtection
90
91 [ v3_ca ]
92 subjectKeyIdentifier=hash
93 authorityKeyIdentifier=keyid:always,issuer:always
94 basicConstraints = CA:true
95
96 [ crl_ext ]
97 authorityKeyIdentifier=keyid:always,issuer:always
98
99 [ engine ]
100 default = openssl
101
```