

```
1 HOME = .
2 RANDFILE = $ENV::HOME/.rnd
3 oid_section = new_oids
4
5 [ new_oids ]
6
7 [ ca ]
8 default_ca = EndianIPSEC
9
10 [ EndianIPSEC ]
11 dir = /var/efw/vpn/ca/
12 certs = $dir/certs
13 crl_dir = $dir/crl
14 database = $dir/certs/index.txt
15 new_certs_dir = $dir/certs
16 certificate = $dir/cacerts/cacert.pem
17 serial = $dir/certs/serial
18 crl = $dir/crl.pem
19 private_key = $dir/private/cakey.pem
20 RANDFILE = $dir/private/.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
29 [ policy_match ]
30 countryName = optional
31 stateOrProvinceName = optional
32 organizationName = optional
33 organizationalUnitName = optional
34 commonName = supplied
35 emailAddress = optional
36
37 [ req ]
38 default_bits = 2048
39 default_keyfile = privkey.pem
40 distinguished_name = req_distinguished_name
41 attributes = req_attributes
42 x509_extensions = v3_ca
43 string_mask = nombstr
44
45 [ req_distinguished_name ]
46 countryName = Country Name (2 letter code)
47 countryName_default = DE
48 countryName_min = 2
49 countryName_max = 2
50
51 stateOrProvinceName = State or Province Name (full name)
52 stateOrProvinceName_default = Niedersachsen
53
54 localityName = Locality Name (eg, city)
55 localityName_default = Loxstedt
56
57 0.organizationName = Organization Name (eg, company)
58 0.organizationName_default = blablaName
59
60 organizationalUnitName = Organizational Unit Name (eg, section)
61 #organizationalUnitName_default =
62
63 commonName = Common Name (eg, your name or your server's hostname)
64 commonName_max = 64
65
66 emailAddress = Email Address
67 emailAddress_max = 40
68
69 [ req_attributes ]
```

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