OpenSSL

! OpenSSL 1.1.0

1. (rtengine) .
2. PKCS#11 .
3. OpenSSL 1.1.0 .
4. OpenSSL (Linux: `/usr/lib/ssl/openssl.cnf` , Windows OpenSSL). :

   openssl_conf = openssl_def

   :

   [openssl_def]

   engines = engine_section

   [engine_section]

   rtengine = gost_section

   [gost_section]

   dynamic_path = /path/to/librtengine.so

   MODULE_PATH = /path/to/librtpkcs11ecp.so

   RAND_TOKEN = pkcs11:manufacturer=Aktiv%20Co.;model=Rutoken%20ECP

   default_algorithms = CIPHERS, DIGEST, PKEY, RAND

   dynamic_path — rtengine.

   MODULE_PATH — librtpkcs11ecp.

   RAND_TOKEN — pkcs11 uri.

   :

   manufacturer: ID ;

   model: ;

   serial: ;

   token: ("label").

   Windows .

5. `OPENSSL_CONF`, .

   Linux, , , bash :

   export OPENSSL_CONF=/path/to/openssl.cnf

   Windows, cmd:

   set OPENSSL_CONF=C:\path\to\openssl.cnf

OpenSSL

```
#   rtengine
openssl_conf = openssl_def

[ openssl_def ]
engines = engine_section

[ engine_section ]
```

```
rtengine = gost_section

[ gost_section ]
dynamic_path = /path/to/librtengine.so
MODULE_PATH = /path/to/librtpkcs11ecp.so
RAND_TOKEN = pkcs11:manufacturer=Aktiv%20Co.;model=Rutoken%20ECP;serial=2adc8d87
default_algorithms = CIPHERS, DIGEST, PKEY, RAND

#
[ req ]
prompt = no
distinguished_name = req_distinguished_name
req_extensions = ext

#
[ req_distinguished_name ]
countryName = RU
commonName = Ivanov
emailAddress = ivanov@mail.ru
stateOrProvinceName = Moscow

#
[ ext ]
subjectSignTool = ASN1:FORMAT:UTF8,UTF8String: \"  2.0\"
extendedKeyUsage=emailProtection
keyUsage=digitalSignature,nonRepudiation,keyEncipherment,dataEncipherment

#
[ ca ]
default_ca = CA_default
[ CA_default ]
dir = ./demoCA #
database = $dir/index.txt
new_certs_dir = $dir/newcerts # ,
certificate = $dir/cacert.pem #
serial = $dir/serial
private_key = $dir/private/cakey.pem #
RANDFILE = $dir/private/.rand
default_days = 365 #
default_crl_days = 30
```

```
default_md = md_gost12_256 #
policy = policy_any
email_in_dn = no
name_opt = ca_default
cert_opt = ca_default
copy_extensions = copy

#
[ policy_any ]
countryName = supplied
stateOrProvinceName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
```