

! OpenSSL 1.0 .

OpenSSL 1.0.1f , 2 engine.

1. (engine pkcs11_gost) .
 2. PKCS#11 .
 3. OpenSSL, engine gost (libgost.so) .
 4. engine pkcs11_gost.
- , pkcs11_gost libpkcs11_gost
5. OpenSSL (Ubuntu: /usr/lib/ssl/openssl.cnf , Windows OpenSSL). :

```
openssl_conf = openssl_def
```

, :

```
[openssl_def]
engines = engine_section

[engine_section]
gost = gost_section
pkcs11 = pkcs11_section

[gost_section]
engine_id = gost
dynamic_path = /usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libgost.so
default_algorithms = ALL
init = 0

[pkcs11_section]
engine_id = pkcs11_gost
dynamic_path = /usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libpkcs11_gost.so
MODULE_PATH = /usr/lib/librtpkcs11lecp.so
init = 0
```

Windows .

6. **dynamic_path** engine (pkcs11_gost libpkcs11_gost). **MODULE_PATH** PKCS#11 .
OPENSSL_CONF

OpenSSL Windows

```
openssl_conf = openssl_def

[ ca ]
default_ca = CA_default # The default ca section

[ CA_default ]
dir = ./demoCA # top dir
database = $dir/index.txt # index file.
new_certs_dir = $dir/newcerts # new certs dir
certificate = $dir/cacert.pem # The CA cert
serial = $dir/serial # serial no file
private_key = $dir/private/cakey.pem# CA private key
RANDFILE = $dir/private/.rand # random number file
default_days = 365 # how long to certify for
default_crl_days = 30 # how long before next CRL
default_md = md_gost94 # md to use
policy = policy_any # default policy
email_in_dn = no # Don't add the email into cert DN
name_opt = ca_default # Subject name display option
cert_opt = ca_default # Certificate display option
copy_extensions = none # Don't copy extensions from request
organizationName = optional
organizationalUnitName = optional
commonName = optional
emailAddress = optional

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

[req]
distinguished_name = req_distinguished_name
prompt = yes

[req_distinguished_name]
ST = State or Province
L =Locality
O = Organization Name
OU = Organizational Unit Name
CN = Common Name
emailAddress = Email

[openssl_def]
engines = engine_section

[engine_section]
gost = gost_section
pkcs11 = pkcs11_section

[gost_section]
engine_id = dynamic
dynamic_path = C:/openssl/engines/gost.dll
init = 0
default_algorithms = ALL

[pkcs11_section]
engine_id = dynamic
dynamic_path = C:/openssl/engines/pkcs11_gost.dll
MODULE_PATH = C:/openssl/engines/rtPKCS11ECP.dll
init = 0
default_algorithms = ALL
```