34.10-2001

```
openssl genpkey -engine pkcs11_gost -algorithm GOST2001 -pkeyopt key_id:50 -pkeyopt paramset:A -pkeyopt pin:
12345678
```

- **key_id** - ID
- **paramset** - :
  - A - OID 1.2.643.2.2.35.1;
  - B - OID 1.2.643.2.2.35.2;
  - C - OID 1.2.643.2.2.35.3;
  - XA - OID 1.2.643.2.2.36.0;
  - XB - OID 1.2.643.2.2.36.1;
- **pin** - PIN-

PKCS#10

```
openssl req -engine pkcs11_gost -new -key 50 -keyform engine -out req.csr
```

PIN-. :

- State or Province []: Moscow
- Locality []: RU
- Organization Name []: Aktiv Company
- Organizational Unit Name []: development
- Common Name []: tester
- Email []: tester@rutoken.ru

openssl.cfg.

CA

, , .

CA:

```
openssl genpkey -engine pkcs11_gost -algorithm GOST2001 -pkeyopt key_id:1000 -pkeyopt paramset:A -pkeyopt pin:
12345678
```

:

```
openssl req -engine pkcs11_gost -x509 -new -key 1000 -keyform engine -out ca.crt
```

- OpenSSL/bin demoCA
- demoCA newcerts
- demoCA index.txt serial ( )
- serial 01. .

:

```
openssl ca -engine pkcs11_gost -keyfile 1000 -keyform engine -cert ca.crt -in req.csr -out tester.crt
```

""

S/MIME:

```
openssl smime -engine pkcs11_gost -sign -in data.file -out data.sig -nodetach -binary -signer tester.crt -inkey
50 -keyform engine
```

PKCS#7:

```
openssl smime -engine pkcs11_gost -sign -in  data.file -out data.sig -nodetach -binary -signer tester.crt -
inkey 50 -keyform engine -outform PEM
```

CMS:

```
openssl cms -engine pkcs11_gost -sign -in data.file -out data.sig -nodetach -binary -signer tester.crt -inkey
50 -keyform engine -outform PEM
```

, “” *-nodetach.*

""

S/MIME:

```
openssl smime -engine pkcs11_gost -verify -in data.sig -inform SMIME -CAfile ca.crt -out data.file
```

PKCS#7:

```
openssl smime -engine pkcs11_gost -verify -in data.sig -inform PEM -CAfile ca.crt -out data.file
```

CMS:

```
openssl cms -engine pkcs11_gost -verify -in data.sig -inform PEM -CAfile ca.crt -out data.file
```

"" 34.10-2001

```
openssl dgst -engine pkcs11_gost -md_gost94 -sign 50 -keyform engine data.file
```

CMS

, . :

```
[pkcs11_section]
engine_id = dynamic
dynamic_path = C:/openssl/engines/pkcs11_gost.dll
MODULE_PATH = C:/openssl/engines/rtPKCS11ECP.dll
PIN = 12345678
init = 0
default_algorithms = ALL
```

PIN, PIN- .

```
openssl smime -engine pkcs11_gost -encrypt -binary -gost89 -in data.file -out data.enc respondent_gost.crt
```

respondent_gost.crt - , .

:

```
openssl smime -decrypt -engine gost -in data.enc -recip respondent_gost.crt -inkey respondent_gost.key -out
data.file
```