rtengine , .

pkcs11 uri.

:

manufacturer: ID

model:

serial:

token: ("label")

object: (CKA_LABEL)

id: (CKA_ID)

:

pkcs11:manufacturer=Aktiv%20Co.;model=Rutoken%20ECP;serial=2adc8d87;object=my%20label;id=%aa%bb%cc%dd

:

pkcs11:model=Rutoken%20ECP

. / .

openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out seckey.pem

, -algorithm.

() -pkeyopt.

:

gost2001: A,B,C,XA,XB

gost2012_256: A,B,C,XA,XB

gost2012_512: A,B

OpenSSL . pkcs11-tool OpenSC.

-2001

pkcs11-tool.exe --module rtPKCS11ECP.dll --login --pin 12345678 --keypairgen --key-type GOSTR3410:A --id 3132

pin: PIN-

id: (CKA_ID) hex ASCII.
id OpenSSL , . : '--id 3132' OpenSSL "pkcs11:id=12".
- **ASCII-**

GOSTR3410:A : 'A' - , B

-2012

pkcs11-tool -2012 GitHub-, OpenSC 0.19.0.

pkcs11-tool.exe --module rtPKCS11ECP.dll --login --pin 12345678 --keypairgen --key-type GOSTR3410-2012-256:B --id 3132

pin: PIN-

id: (CKA_ID) hex ASCII.
id OpenSSL , .
: '--id 3132' OpenSSL "pkcs11:id=12".
, - ACSII- .

GOSTR3410-2012-512:A : 'A' -, B ,

GOSTR3410-2012-256:B : 'B' -, C D

-" "

:

pkcs11-tool.exe --module rtPKCS11ECP.dll -Ol

PKCS#10

:

openssl req -utf8 -new -key seckey.pem -out req.csr

:

openssl req -utf8 -new -keyform engine -key "pkcs11:your_pkcs11_uri" -engine rtengine -out req.csr

-key " "

PIN-. :

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

openssl.cnf.

:

openssl req -utf8 -x509 -key seckey.pem -out cert.cer

:

openssl req -utf8 -x509 -keyform engine -key "pkcs11:your_pkcs11_uri" -engine rtengine -out cert.cer

CMS

CMS . sdk\openssl\rtengine\samples\tool\ OpenSSL, .

sdk\openssl\rtengine\samples\tool\demoCA openssl.cnf OpenSSL :

openssl ca -batch -in req.csr -out cert.cer

CMS :

openssl cms -sign -binary -nosmimecap -in data_to_sign -out signed_cms -outform PEM -inkey seckey.pem -signer cert.cer

:

openssl cms -sign -binary -nosmimecap -in data_to_sign -out signed_cms -outform PEM -keyform engine -inkey "pkcs11:your_pkcs11_uri" -engine rtengine -signer cert.cer

-nodetach CMS — . «».

-nocerts CMS .

CMS

openssl cms -verify -binary -in signed_cms -inform PEM -out verified_data -CAfile demoCA/cacert.pem -content data_to_sign

, -CAfile,

.

-content , CMS .

CMS ( ), -certfile.

«»

:

openssl dgst -sign seckey.pem -out signature data_to_sign

:

openssl dgst -keyform engine -sign "pkcs11:your_pkcs11_uri" -engine rtengine -out signature data_to_sign

.

« »

:

openssl pkey -in seckey.pem -pubout -out pubkey.pem

:

openssl dgst -verify pubkey.pem -signature signature data_to_sign

:

openssl dgst -keyform engine -verify "pkcs11:your_pkcs11_uri" -engine rtengine -signature signature test_data

CMS

openssl cms -encrypt -binary -gost28147-paramset_a-cfb -in test_data -out encrypted_cms -outform PEM respondent.cer

respondent.cer: , .

gost28147-paramset_a-cfb: , .

:

:

openssl cms -decrypt -binary -in encrypted_cms -inform PEM -recip respondent.cer -inkey seckey.pem -out decrypted_cms_data

:

openssl cms -decrypt -binary -in encrypted_cms -inform PEM -recip respondent.cer -keyform engine -inkey "pkcs11:your_pkcs11_uri" -engine rtengine -out decrypted_cms_data

SSL/TLS /

, :

openssl s_server -key demoCA/private/cakey.pem -cert demoCA/cacert.pem -Verify 7 -CAfile demoCA/cacert.pem -accept 44330 -WWW -purpose any -4

, :

```
openssl s_server -keyform engine -key "pkcs11:server_key_pkcs11_uri" -engine rtengine -cert demoCA/cacert.
pem -Verify 7 -CAfile demoCA/cacert.pem -accept 44330 -WWW -purpose any -4
```

, :

```
openssl s_client -host 127.0.0.1 -port 44330 -cert cert.cer -key seckey.pem
```

, :

```
openssl s_client -host 127.0.0.1 -port 44330 -cert cert.cer -keyform engine -key "pkcs11:
client_key_pkcs11_uri" -engine rtengine
```