

v1.22_ 34.10-2012

1 2020 RSA- 34.10-2012. - .
(openssl, bouncycastle) . PKCS#12 OpenSSL :

```
$ openssl pkcs12 -in container.pfx
Enter Import Password:
Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: 20200313-114830-# ! (/) " &"-!" 2012
    Microsoft CSP Name: Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider
Error outputting keys and certificates
140403870810560:error:06074079:digital envelope routines:EVP_PBE_CipherInit:unknown pbe algorithm:../crypto/evp
/evp_pbe.c:95:TYPE=1.2.840.113549.1.12.1.80
140403870810560:error:23077073:PKCS12 routines:PKCS12_pbe_crypt:pkcs12 algor cipherinit error:../crypto/pkcs12
/p12_decr.c:41:
140403870810560:error:2306A075:PKCS12 routines:PKCS12_item_decrypt_d2i:pkcs12 pbe crypt error:../crypto/pkcs12
/p12_decr.c:94:
```

OpenSSL

OpenSSL 1.1.1 11 Sep 2018 Ubuntu 18.04.



Docker OpenSSL + Gost engine.

docker- OpennSSL + Gost engine: <https://hub.docker.com/r/rnix/openssl-gost/>

gost engine:

```
apt install libengine-gost-openssl1.1
```

openssl: /etc/ssl/openssl.cnf:

:

/etc/ssl/openssl.cnf

openssl_conf = openssl_def

:

/etc/ssl/openssl.cnf

```
[openssl_def]
engines = engine_section
[engine_section]
gost = gost_section
[gost_section]
default_algorithms = ALL
engine_id = gost
CRYPTO_PARAMS = id-Gost28147-89-CryptoPro-A-ParamSet
```

- :

```
openssl ciphers | tr ":" "\n" | grep -i gost
```

GOST2012, .

PKCS#12

, :

```
header.key  
masks2.key  
masks.key  
name.key  
primary2.key  
primary.key
```

:

```
docker run --rm -i -t -v `pwd`:`pwd` -w `pwd` rnix/openssl-gost bash
```

get-cpcert-bin.tar.gz: <https://github.com/kov-serg/get-cpcert/releases/download/v1.0.1/get-cpcert-bin.tar.gz>

get-cpcert-bin , ;

docker-:

```
./get-cpcert <PATH> <PASSWORD> > result.pem
```

<PATH> — , , <PASSWORD> — . result.pem, .

PKCS#12, :

```
openssl pkcs12 -engine gost -export -in result.pem -out result.pfx
```

result.pfx . 1.11 1.15+.