

- [libgost-astra](#)
- [openssl](#)



:

- Astra Linux Special Edition .10015-01 (1.7), .10015-10
- Astra Linux Special Edition .10015-17
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10015-03 (7.6)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1
- Astra Linux Special Edition .10015-16 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12

libgost-astra

Astra Linux



libgost-astra

, openssl openvpn, :

- 34.10-2001 34.10-2012 - . , (. RFC 4357). :
 - 256 2001, 256/512 2012;
 - 512 2001 512/1024 2012;
- 34.11-94 . 256 ;
- 34.11-2012 . 256 512 ;
- 28147-89 - 256 . CBC, CFB CNT, "key meshing" (RFC 4357);
- 28147-89 . . 256 8 64 (32);
- 34.13-2015 - "" ("Grasshopper").

[synaptic](#),

```
apt install libgost-astra
```

openssl (/etc/ssl/openssl.cnf).

openssl genpkey, :

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

-algorithm , -pkeyopt . :

gost2001	0, A, B, C, XA, XB
gost2012_256	
gost2012_512	A, B

```
openssl engine gost -c
```

openssl



libgost-astrs . . .

libgost-astra /etc/ssl/openssl.cnf



openssl_conf = openssl_def



```
[openssl_def]
engines = engine_section

[engine_section]
gost-astra = gost_section

[gost_section]
engine_id = gost-astra
dynamic_path = <>
default_algorithms = ALL
CRYPT_PARAMS = id-Gost28147-89-CryptoPro-A-ParamSet
```

[gost_section]:

engine_id = gost-astra	(- engine). gost-astra. openssl engine libgost-astra : # openssl engine (rdrand) Intel RDRAND engine (dynamic) Dynamic engine loading support (gost-astra) Astra implementation of GOST engine
dynamic_path = <>	, . . . openssl . . . : dpkg -L libgost-astra grep engines
default_algorithms = ALL	, . . . openssl engine gost -c libgost-astra : # openssl engine gost-astra -c (gost-astra) Astra implementation of GOST engine [gost89, gost89-cnt, gost89-cnt-12, gost89-cbc, grasshopper-ecb, grasshopper-cbc, grasshopper-cfb, grasshopper-ofb, grasshopper-ctr, md_gost94, gost-mac, md_gost12_256, md_gost12_512, gost-mac-12, gost2001, gost-mac, gost2012_256, gost2012_512, gost-mac-12]

CRYPT_PARAMS = id-
Gost28147-89-
CryptoPro-A-ParamSet

CRYPT_PARAMS gost-astra.
.
-gost89, , , **GOST 28147-89 rc2-cbc.**