

Astra Linux:

- -
- `digsig_verif`
 - `fly-admin-smc`
 - `astra-digsig-control`
 - `/etc/digsig/`
 - `/etc/digsig/digsig_initramfs.conf`
 -
 -
-
- `fly-admin-smc`
- -
 -



:

- Astra Linux Special Edition .10015-01 (1.7) 5.4
- Astra Linux Special Edition .10015-01 (1.6) 5.4
- Astra Linux Special Edition .10015-16 . 1



5.4 , .

() () . Astra Linux (digsig_verif), () . :

- `ELF () - , (-);`
- `- , (-);`

.

ELF, , . .

() ():

1. (bash). . `astra-interpreters-lock` `astra-safepolicy.` , , .
2. `bash.`
3. .
4. `-2 -2 (. -2: parsec-kiosk2 ().`

:

:

1. (bash).:

```
sudo astra-interpreters-lock enable
```

2. `bash.:`

```
sudo astra-bash-lock enable
```

3. `..:`

```
sudo astra-nochmodx-lock enable
```

4. :

- a. (bash):

```
sudo astra-interpreters-lock status
```

```
"" ;
```

```
sudo astra-interpreters-lock is-enabled
```

```
"" .
```

b. bash:

```
sudo astra-bash-lock status
```

```
"" ;
```

```
sudo astra-bash-lock is-enabled
```

```
"" .
```

c. :

```
sudo astra-nochmodx-lock status
```

```
"" ;
```

```
sudo astra-nochmodx-lock is-enabled
```

```
"" .
```

5. -2

a. -2.:

```
echo 1 | sudo tee /sys/module/parsec/parameters/uc_enforce
```

b. .:

```
echo 1 | sudo tee /sys/module/parsec/parameters/uc_complain;
```

c. -2 .:

```
echo 1 | sudo tee /etc/parsec/kiosk2_enforce; echo 1 | sudo tee  
/etc/parsec/kiosk2_complain;
```

:

1. : - - - :

```
sudo fly-admin-smc
```

2. :

— .

3. :

a. " Bash ".

b. " Bash ".

4. .

5. , " , ":

— .

:

• :

```
sudo reboot
```

• — — .

digsig_verif

fly-admin-smc

fly-admin-smc . fly-admin-local, :<< — — — >>. . fly-admin-smc fly-admin-digsig .


astra-digsig-control

astra-digsig-control [astra-safepolicy](#). .

/etc/digsig/

/etc/digsig/digsig_initramfs.conf

/etc/digsig/digsig_initramfs.conf.

 , , /etc/digsig (— , /etc/digsig/digsig_initramfs.conf) :

1. :

```
sudo update-initramfs -u -k all
```

2. .

 , /etc/digsig , .

:

<_>=<_>

:

- DIGSIG_ELF_MODE — ELF. :
 - 0 — . . ;
 - 1 — . . , , ;
 - 2 — . . , , ;
- DIGSIG_XATTR_MODE — . :
 - 0 — . . ;
 - 1 — . . , , ;
 - 2 — . . , , ;
- DIGSIG_IGNORE_XATTR_KEYS — :
 - 0 — . ;
 - 1 — ;
- DIGSIG_IGNORE_GOST2001 — ~~34.10-2001:
 - 0 — . ~~34.10-2001 ;
 - 1 — ~~34.10-2001 ;

/etc/digsig/digsig_initramfs.conf /etc/digsig/ :

- /etc/digsig/keys — ;
- /etc/digsig/xattr_control — , , ;
- /etc/digsig/xattr_keys — , ;

/etc/digsig/xattr_control , , . :

- , . slash (, "/");
- , slash ("/"), . : /bin/script.sh;
- , slash, , () . : /bin/;
- , , /bin/script : /bin/script, /bin/script.signed, /bin/script12345 ..

sysfs. :

- , , , ramfs . /etc/digsig ;
- (");
- , .. ("");
- (,) , ;
- , , ;
- , , ;

, :

- :
 - /sys/digsig/elf_mode — . DIGSIG_ELF_MODE.



1, , . :

```
sudo cp /etc/digsig/build_system_rbt_root_key_2018.gpg /sys
/digsig/keys
```

- /sys/digsig/xattr_mode — . DIGSIG_XATTR_MODE;
- /sys/digsig/ignore_gost2001 — ~~34.10-2001. DIGSIG_IGNORE_GOST2001;
- /sys/digsig/ignore_xattr_keys — . DIGSIG_IGNORE_XATTR_KEYS;

- :
 - /sys/digsig/keys — ;
 - /sys/digsig/xattr_control — , ;
 - /sys/digsig/xattr_keys — , ;

, , :

```
sudo cat /sys/digsig/<_>
```

, :

```
sudo cat /sys/digsig/elf_mode /sys/digsig/xattr_mode
```

digsig_verify , :

- ;
- ;
- , /etc/digsig/keys.

:

- , — ;
- /etc/digsig/keys () — ;
- /etc/digsig/keys_xattrs () — , , . ..

(.). gnupg --export/etc/digsig/keys ;

. , , .

, , , /etc/digsig/keys/ /etc/digsig/xattr_keys, , :

```
sudo cp /<>/< > /etc/digsig/keys/
```

/etc/digsig/keys . , , :

- (/etc/digsig/keys) digsig_verify ;

```

i /etc/digsig/keys/key1.gpg — 1, ;
  /etc/digsig/keys/key2.gpg — 2, ;
  /etc/digsig/keys/key1/key1-1.gpg — , 1
  /etc/digsig/keys/key1/key1-2.gpg — , 1
  /etc/digsig/keys/key2/key2-1.gpg — , 2
  /etc/digsig/keys/key2/key2-2.gpg — , 2

```

, , /etc/digsig/xattr_keys/ :

```
sudo cp /<>/< > /etc/digsig/xattr_keys/
```

/etc/digsig/xattr_keys/ , . , (.).

fly-admin-smc

Astra Linux fly-admin-smc, : "" - "" - "" - "" - "" . (F1).

ELF

, . GNU Privacy Guard. Astra Linux GnuPG ~34.11-94. :

```
gpg --version
```

1. . .gnupg . fly-admin-smc, .

! RSA. Astra Linux . Astra Linux GOST_R34.10-2012.

a. gpg :

```
gpg --full-generate-key
```

GOST_R34.10-2012. :

```
pub  gP256 2024-03-12 [SC]
     566F70D5D822D1B51B23CBE60055EBA236DA8851
uid                                     Astra Linux <info@astralinux.ru>

```

- , 566F70D5D822D1B51B23CBE60055EBA236DA8851. ;

b. :
i. ,:

```
Key-Type:GOST_R34.10-2012
%no-protection
Name-Real:<_>
Name-Comment: <>
Name-Email: <e-mail>

```

- . Unattended GPG key generation;
ii. :

```
gpg --gen-key --batch <____>
```

- iii. :

```
gpg --list-keys
```

2. :

```
gpg --export <_> | sudo gpg --import  
sudo gpg --sign-key <_>
```

/etc/digsig/xattr_keys.:

```
sudo gpg --export <_> | tee /etc/digsig/xattr_keys/<____>
```



- . :

```
gpg --export <_> | sudo tee /etc/digsig/xattr_keys/<____>
```

3. /etc/digsig/xattr_control ,:

```
/bin/spo
```

"/", , .

4. :



- , .

```
bsign --sign --xattr <_>
```

bsign;

5. :

- a. DIGSIG_XATTR_MODE /etc/digsig/digsig_initramfs.conf, ;
b. :

```
sudo update-initramfs -u -k all
```

- c. ;

bsign:

```
bsign -w <_>
```

digsig_verif . . :

```
sudo dmesg
```

, digsig_verif:

```
sudo dmesg | grep DIGSIG
```

, /var/log/messages /var/log/kernel.log, :

```
... DIGSIG: [ERROR] NOT SIGNED: path=....
```