Ubuntu/Debian (PAM,PKCS15)

1. USB- .
2. USB- :

```
$ lsusb
```

USB-:

```
[dmitrieva@localhost ~]$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 004: ID 0a89:0030 Aktiv Rutoken ECP
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
```

, : **Aktiv Rutoken ECP**

Pluggable Authentication Modules (PAM,) — , API. , .

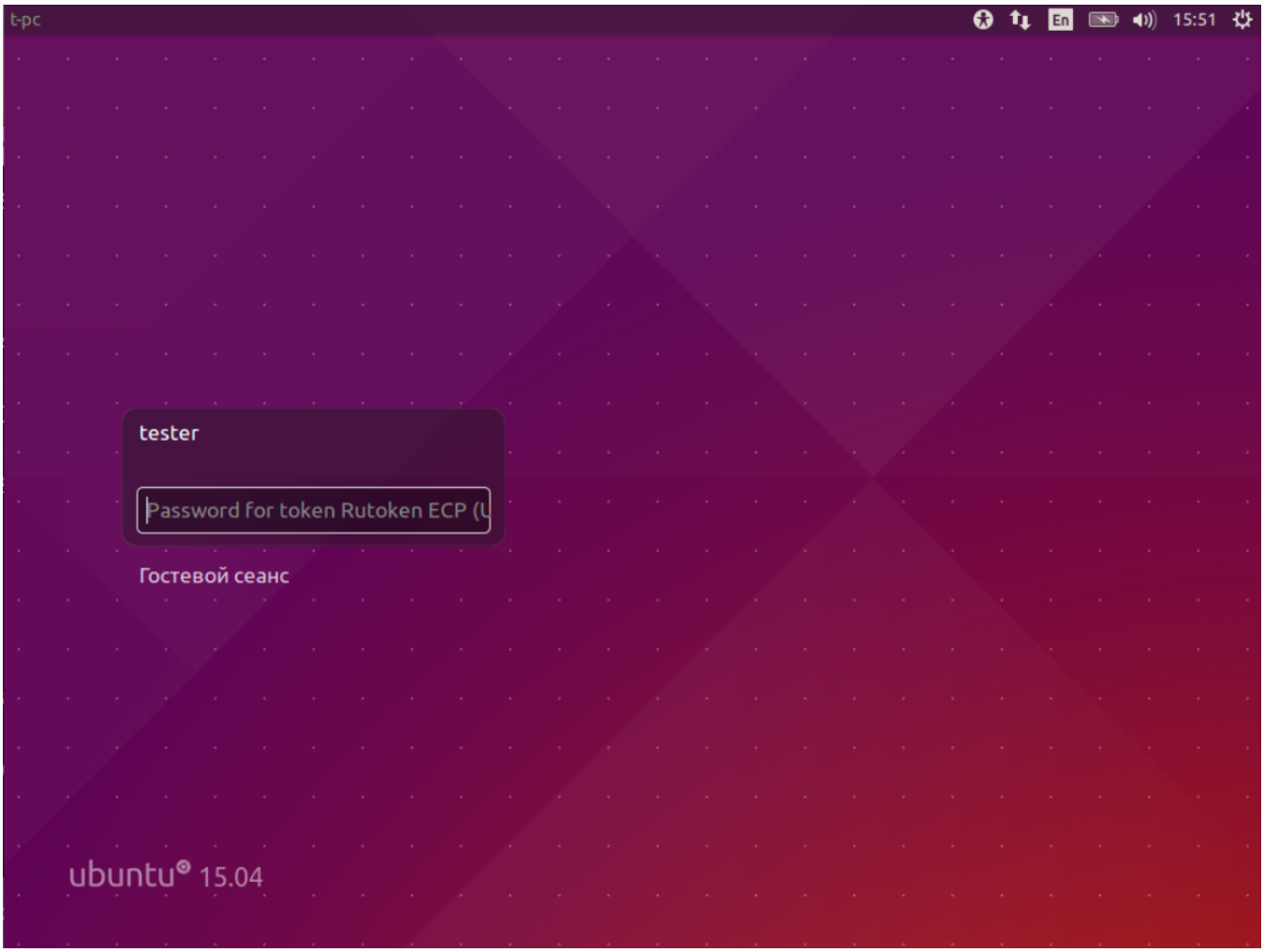
PAM pam_p11, OpenSC, . :

1. `pam_p11_openssh`: ssh `~/.ssh/authorized_keys`
2. `pam_p11_opensc`: `~/.eid/authorized_certificates`

OpenSC pam_pkcs11, .
pam_p11, . , pam_p11 , OCSP. , pam_pkcs11 (,). Gentoo ().
PAM :

1. RSA (, 2048 , 1024)
2. , OpenSSL
3.

:



Ubuntu 18.04. Ubuntu , Debian.

PAM :

- `pcscd`
- OpenSC
- OpenSSL
- libpam-p11
- libengine-pkcs11-openssl

```
sudo apt-get install pcscd opensc openssl libpam-p11 libengine-pkcs11-openssl
```

S .

pam_p11

pam_p11:

1. `/usr/share/pam-configs/p11` :

```
Name: Pam_p11
Default: yes
Priority: 800
Auth-Type: Primary
Auth: sufficient pam_p11_opensc.so /usr/lib/x86_64-linux-gnu/opensc-pkcs11.so
```

Ubuntu 18.04, opensc-pkcs11.so. , ,
/usr/lib/opensc-pkcs11.so. find

2. PAM:

```
sudo pam-auth-update
```

3. , pam_p11. , Unix authentication.

4. .

```
$ pkcs15-init -E
$ pkcs15-init --create-pkcs15 --so-pin "87654321" --so-puk ""
$ pkcs15-init --store-pin --label "User PIN" --auth-id 02 --pin "12345678" --puk "" --so-pin "87654321"
--finalize
```

pin so-pin - .

5. RSA 2048 c ID "45" (id ,). .

```
$ pkcs15-init --generate-key rsa/2048 --auth-id 02 --id 45
< PIN >
```

6. :

```
$ pkcs15-tool --list-keys
Using reader with a card: Aktiv Rutoken ECP 00 00
Private RSA Key [Private Key]
 Object Flags : [0x3], private, modifiable
 Usage : [0x4], sign
 Access Flags : [0x1D], sensitive, alwaysSensitive, neverExtract, local
 ModLength : 2048
 Key ref : 1 (0x1)
 Native : yes
 Path : 3f0010001000600200001
 Auth ID : 02
 ID : 45
```

7. openssl

```
$ sudo openssl
```

8. pkcs11:

```
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1/pkcs11.so -pre ID:pkcs11 -pre
LIST_ADD:1 -pre LOAD -pre MODULE_PATH:/usr/lib/x86_64-linux-gnu/opensc-pkcs11.so
(dynamic) Dynamic engine loading support
[Success]: SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1/pkcs11.so
[Success]: ID:pkcs11
[Success]: LIST_ADD:1
[Success]: LOAD
[Success]: MODULE_PATH:/usr/lib/x86_64-linux-gnu/opensc-pkcs11.so
Loaded: (pkcs11) pkcs11 engine
OpenSSL>
```

9. Ubuntu 18.04, pkcs11.so. , , /usr/lib/openssl/engines/ . find PEM-:

```
OpenSSL> req -engine pkcs11 -new -key 0:45 -keyform engine -x509 -out cert.pem -text
```

10. 0:45 - slot:id (.5). OpenSSL PIN- . , , USB- - . . cert.pem.
: OpenSSL -x509, .

```
verify -CAfile cert.pem cert.pem
cert.pem: OK
```

OpenSSL.

```
exit
```

11. :

```
$ pkcs15-init --store-certificate cert.pem --auth-id 02 --id 45 --format pem
< PIN >
```

12. ID (- 45) :

```
mkdir ~/.eid
chmod 0755 ~/.eid
pkcs15-tool -r <certificate_id> > ~/.eid/authorized_certificates
chmod 0644 ~/.eid/authorized_certificates
```

Ubuntu .

. -, " " .