2FA в IPA (ALSE17)

На стороне клиента

```
sudo mount /dev/sdb1 /mnt/
sudo cp -v /mnt/rutoken_pub.key /etc/digsig/keys/cyberprotect_pub.key && \
sudo update-initramfs -u -k all && \
sudo apt install libccid pcscd libpcsclite1 pcsc-tools opensc libengine-
pkcs11-openssl1.1 -y && \
sudo apt install -f /mnt/librtpkcs11ecp_2.17.1.0-1_amd64.deb
```

```
sudo apt install csp-monitor libnss3-tools krb5-pkinit
sudo mkdir /etc/systemd/system/pcscd.service.d/
sudo tee /etc/systemd/system/pcscd.service.d/override.conf << EOF
[Service]
ExecStart=
ExecStart=/usr/sbin/pcscd --foreground
EOF
```

```
sudo systemctl daemon-reload
sudo systemctl restart pcscd.service
```

```
sudo sed -i -e "/\[pam\]/a pam_cert_auth = True\nresponder_idle_timeout = 0"
/etc/sssd/sssd.conf
```

Добавить в секцию домена:

```
krb5_ccname_template = KEYRING:persistent:%{uid}
```

```
sudo tee -a /etc/sssd/sssd.conf << EOF
[certmap/{{ server.domain }}/rule]
matchrule = <ISSUER>CN={{ defaults.ipa_ca_name }}
maprule = (userCertificate;binary={cert!bin})
EOF
```

```
sudo mkdir /etc/sssd/pki/
sudo cp -v /etc/ipa/ca.crt /etc/sssd/pki/sssd_auth_ca_db.pem
```

```
sudo mkdir -p /etc/pkcs11/modules
echo -e "module: /usr/lib/librtpkcs11ecp.so" | sudo tee
/etc/pkcs11/modules/a-rutoken.module
echo -e "module: /usr/lib/librtpkcs11ecp.so" | sudo tee /usr/share/p11-
kit/modules/a-rutoken.module
p11-kit list-modules
```

Настройка PAM-стека

```
sudo pam-auth-update --remove astra-sss-2fa astra-sss-2fa-try astra-sss-2fa-require sss sss-smart-card-optional sss-smart-card-required
sudo DEBIAN_FRONTEND=noninteractive pam-auth-update --enable astra-sss-2fa-require
sudo systemctl restart sssd
```

CSP-Monitor

```
sudo tee /etc/security/pam_csp.conf << EOF
[global]
pkcs11_module = librtpkcs11ecp.so
EOF
sudo systemctl restart csp-monitor
```

```
sudo touch /var/lib/sss/pubconf/pam_preauth_available
```

На стороне сервера

Настройка XCA для работы с интерфейсной библиотекой

```
sudo mount /dev/sdb1 /mnt/
sudo cp -v /mnt/rutoken_pub.key /etc/digsig/keys/cyberprotect_pub.key && \
sudo update-initramfs -u -k all && \
sudo apt install libccid pcscd libpcsclite1 pcsc-tools opensc libengine-pkcs11-openssl1.1 -y && \
sudo apt install -f /mnt/librtpkcs11ecp_2.17.1.0-1_amd64.deb
```

Выпустить при помощи XCA сертификат пользователя

From:
https://wiki.virtlab.space/ -

Permanent link:
https://wiki.virtlab.space/russianway:alse_ipa2fa

Last update: **2025/04/11 18:24**