КриптоПро: IFCP plugin для входа ЕСИА (Госуслуги)

Про ifcp плагин

Для доступа к Госуслугам был использован Рутокен ЭЦП 2, «КриптоПро 4.0 R4», Chromium browser 72, IFCP-plugin 3.0.6.0

> IFCP plugin работает с КриптоПро версией 4r4 и выше.

Установка плагина для работы с порталом государственных услуг

Для аутентификации через ЕСИА esia.gosuslugi.ru следует:

1) Скачать IFCP-плагин с сайта ГосУслуг в формате «deb» — файл IFCPlugin-x86_64.deb; https://ds-plugin.gдобавитьosuslugi.ru/plugin/upload/Index.spr

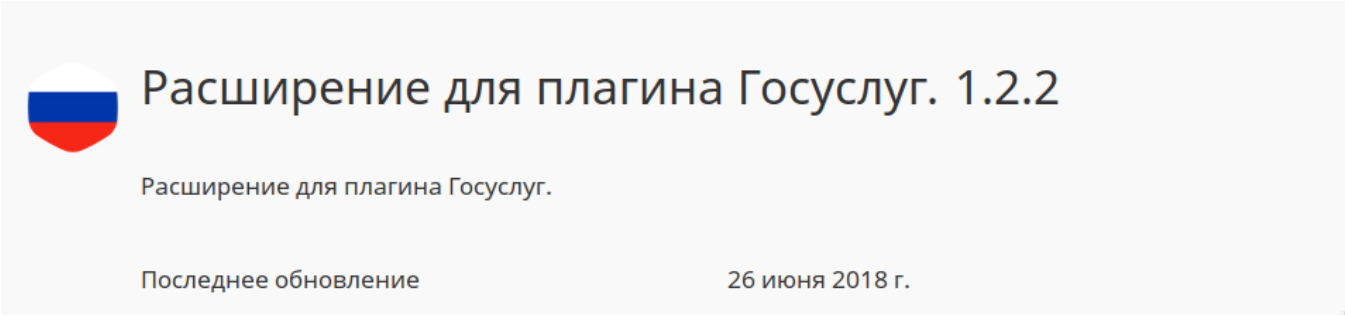
Linux LSB 3.6/4.0 (deb-based), 32-bit	IFCPlugin-i386.deb
Linux LSB 3.6/4.0 (deb-based), 64-bit	IFCPlugin-x86_64.deb

2) Установить плагин:

```
$ sudo dpkg -i IFCPlugin-x86_64.deb
```

3) Добавить расширение для Госуслуг в браузере chromium:

Расширение для chromium



4) Для правильной работы плагина, следует прописать символические ссылки:

Для браузера Chromium:

```
sudo ln -s /etc/opt/chrome/native-messaging-hosts/ru.rtlabs.ifcplugin.json /etc/chromium/native-messaging-hosts
```

Для браузера Mozilla Firefox:

```
sudo ln -s /opt/cprocsp/lib/amd64/libcppkcs11.so.4.0.4 /usr/lib/mozilla/plugins/lib/libcppkcs11.so
```

Примечание: libcppkcs11.so.4.0.X может отличаться, в зависимости от версии КриптоПро CSP.

Настройка конфигурационных файлов

5) Добавить в конфигурационный файл IFCplugin /etc/ifc.cfg :

Для ifc plugina версии 3.0.4.0 - 3.0.7.0 конфигурационный файл следует заменить на:

```
log = {
    level = "DEBUG";
}

config = {
    cert_from_registry = "false";
    set_user_pin = "false";
}

params =
(
    {
        name = "CPPKCS11_2001";
        alias = "CPPKCS11_2001";
        type = "pkcs11";
        alg = "gost2001";
        model = "CPPKCS 3";
        lib_linux = "libcppkcs11.so";
    },
    {
        name = "CPPKCS11_2012_256";
        alias = "CPPKCS11_2012_256";
        type = "pkcs11";
        alg = "gost2012_256";
        model = "CPPKCS 3";
        lib_linux = "libcppkcs11.so";
    },
    {
        name = "CPPKCS11_2012_512";
        alias = "CPPKCS11_2012_512";
        type = "pkcs11";
        alg = "gost2012_512";
        model = "CPPKCS 3";
        lib_linux = "libcppkcs11.so";
    }
);
```

Можно воспользоваться готовым конфигурационным файлом от КриптоПро для ifcp plugin:

https://www.cryptopro.ru/sites/default/files/public/faq/ifcx64.cfg

Например:

wget https://www.cryptopro.ru/sites/default/files/public/faq/ifcx64.cfg
$ sudo rm /etc/ifc.cfg
$ sudo cp ~/ifcx64.cfg /etc/ifc.cfg
$ /opt/cprocsp/bin/amd64/csptestf -absorb -certs -autoprov

6) В КриптоПро CSP для корректной работы pkcs11, настройку слотов следует сделать явной:

Для этого в конфигурационный файл /etc/opt/cprocsp/config64.ini следует в разделе PKCS11 добавить:

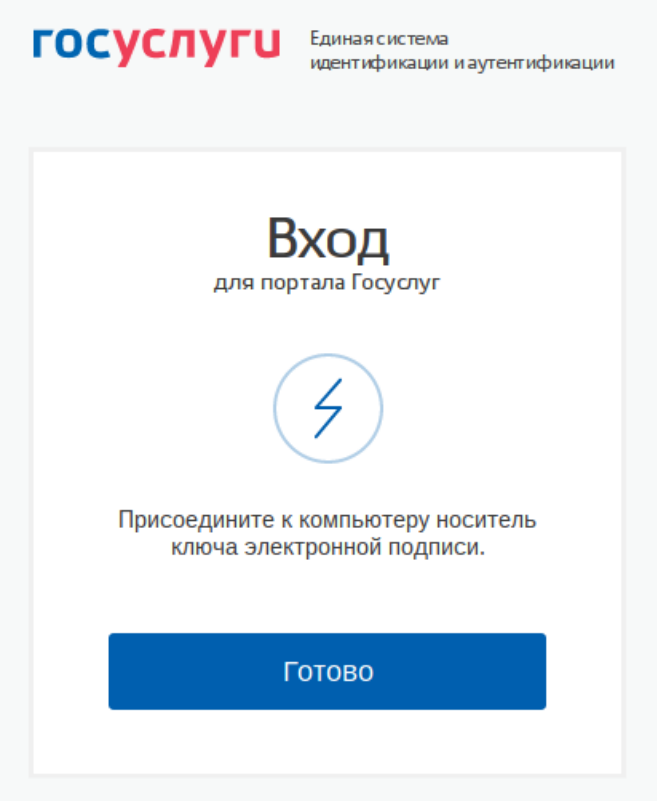
```
# [PKCS11\slot0]
# ProvGOST = "Crypto-Pro GOST R 34.10-2001 KC1 CSP"
# ProvRSA = "Microsoft Strong Cryptographic Provider"
# reader = hdimage


[PKCS11\slot17]
ProvGOST = "Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider"
Firefox = 1
Reader = ""
```

Просмотр логов

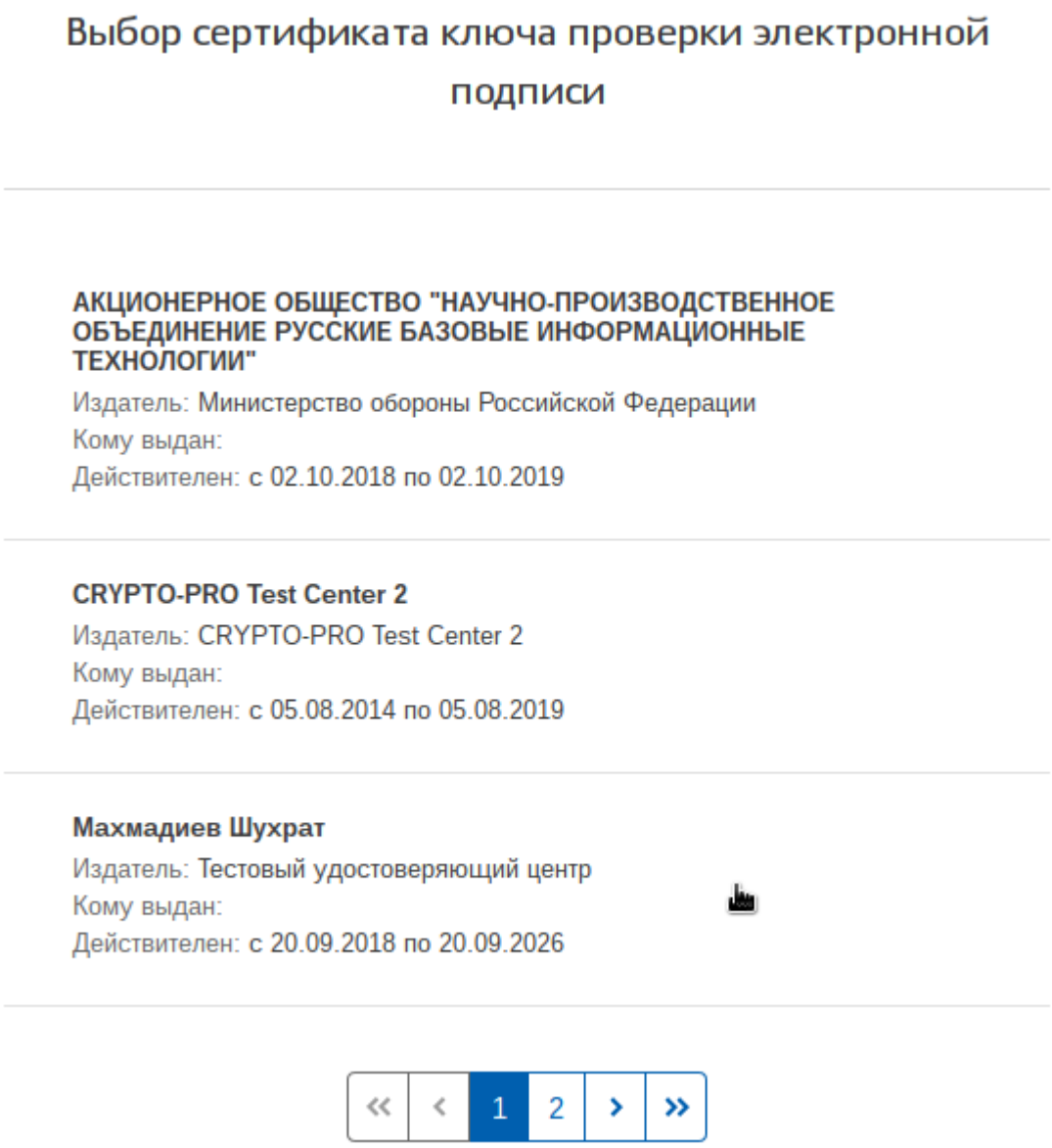
7) Для проверки работы плагина, в терминале в режиме live можно просмотреть логи:

```
tail -f /var/log/ifc/engine_logs/engine.log
```

8) Для авторизации следует пройти по адресу: esia.gosuslugi.ru и выбрать Вход с помощью электронной подписи



9) Подключив токен, следует нажать кнопку "Готово", после чего система предложит выбрать нужный сертификат ключа проверки ЭЦП:



Убедитесь, что Ваш личный сертификат добавлен (с привязкой к закрытому ключу) в хранилище пользователя uMy.

Инструкция: Менеджер сертификатов КриптоПРО в Linux

Возможные ошибки

В случае если после ввода pin-кода, браузер возвращает Вас в окно выбора сертификата, следует проверить, что личный сертификат пользователя находится внутри контейнера ключей. Критично для версии КриптоПро 4r4.

Для записи сертификата в контейнер можно воспользоваться командой:

```
/opt/cprocsp/bin/amd64/csptest -keys -cont '_' -keytype exchange -impcert /tmp/_.cer
```

Список ГИС и ЭТП использующих cades-bes plugin

ЭЦП в государственных информационных системах и электронно торговых площадках

Перечень аккредитованных удостоверяющих центров

Портал уполномоченного федерального органа в области использования электронной подписи с перечнем сертификатов аккредитованных удостоверяющих центров России:

https://e-trust.gosuslugi.ru/CA/

Подтверждение подлинности ЭП на сайте госуслуг

Данный сервис предназначен для подтверждения подлинности ЭП сертификатов в форматах X.509 и BASE64.

Можно подтвердить подлинность ЭП сертификата, изданного удостоверяющим центром, входящим в список аккредитованных удостоверяющих центров Министерства связи и массовых коммуникаций.

https://www.gosuslugi.ru/pgu/eds