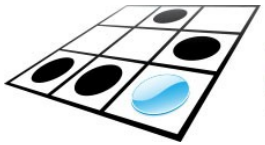
Федеральная служба судебных приставов

Управление информационных технологий

Криптографические операции в окружении рабочего стола ОС «Гослинукс»

Б.В. Макаренко
Консультант отдела обеспечения информационной безопасности



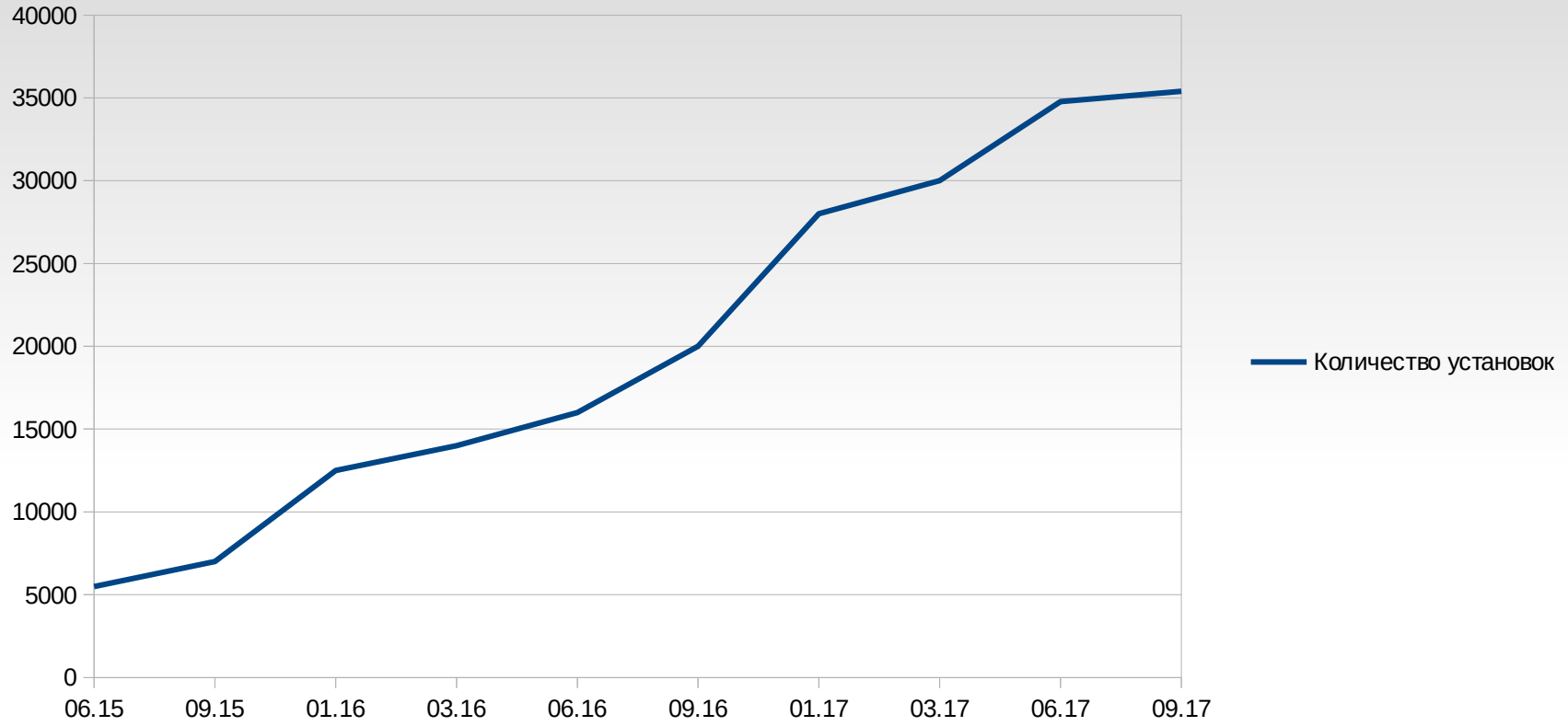
XIV Конференция разработчиков свободных программ

Калуга
2017

Операционная система типового дистрибутива АИС ФССП России

- Отечественная
- Защищенная
- На базе СПО
- Бесплатная

Показатель внедрения ОС «Гослинукс» в ТО ФССП России



По состоянию на сентябрь 2017 г. в 62-ти Территориальных органах ФССП России ОС Гослинукс была установлена на 70 и выше процентов от числа средств вычислительной техники.

В планах на 2017 год обеспечить внедрение ОС Гослинукс до 90% во всех ТО.

token-manager

Графический интерфейс управления
ключевыми носителями и сертификатами

token-manager

В чем была проблема?

```
# sudo -u fssp ./csptest -keyset -enum_cont -fqcn -verifyc
CSP (Type:75) v3.6.5360 KC1 Release Ver:3.6.7092 OS:Linux CPU:AMD64 FastCode:READY,ENABLED.
AcquireContext: OK. HCRYPTPROV: 38874819
\\.\Aktiv Rutoken S 00 00\RaUser-91ac5c9c-f655-452c-a12b-3b5dc763f149
OK.
Total:
[ErrorCode: 0x00000000]

# sudo -u fssp ./certmgr -inst -cont '\\.\Aktiv Rutoken S 00 00\RaUser-91ac5c9c-f655-452c-a12b-3b5dc763f149'
Certmgr 0.9 prerelease (c) "CryptoPro", 2007-2010.
program for managing certificates, CRLs and stores

Install:
================================================================================
1-------
Issuer: CN=УЦ ФССП России
Subject    : 1.2.643.5.1.5.2.1.1="#13053037303030", OGRN=1040700234300, INN=0721009673, E=mail@r07.fssprus.ru,
C=RU, S=Кабардино-Балкарская Республика, L=Нальчик, O=УФССП России по Кабардино-Балкарской Республике, OU=УФССП
России по Кабардино-Балкарской Республике, CN=ВУЦ07000, STREET="ул. И.Арманд, 43а",
1.2.840.113549.1.9.2= "#1E18041E043F043504400430044204300E0440020041204230426", I=B.B., G=ВУЦ, SN=ВУЦ
Serial: 0xAF3400000200C4006C2A
SHA1 Hash: 0x76aeec5e48214af8fce61baf863d2452ce8c9ba8
Not valid before: 20/11/2012  11:26:00 UTC
Not valid after: 20/02/2014  11:36:00 UTC
PrivateKey Link: Yes. Container: SCARD\rutoken_2ae854b4\0A00\6C3F
================================================================================

[ErrorCode: 0x00000000]
```

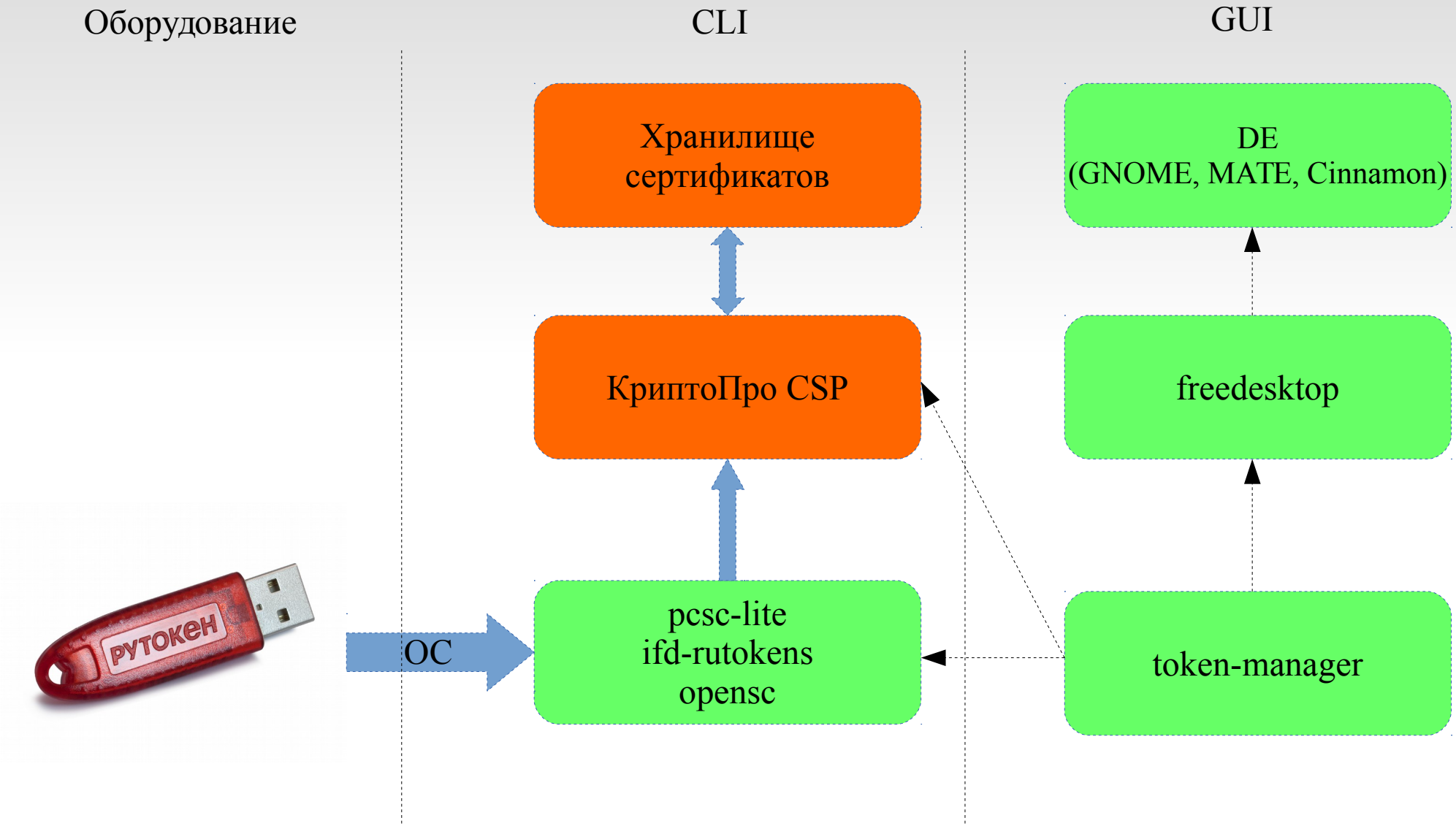
token-manager

Возможности

- Просмотр подключенных ключевых носителей (токенов)
- Просмотр сертификатов в контейнерах на ключевом носителе
- Просмотр сертификатов в корневом и личном хранилищах
- Установка корневых сертификатов и списков отозванных сертификатов
- Установка лицензии КриптоПро

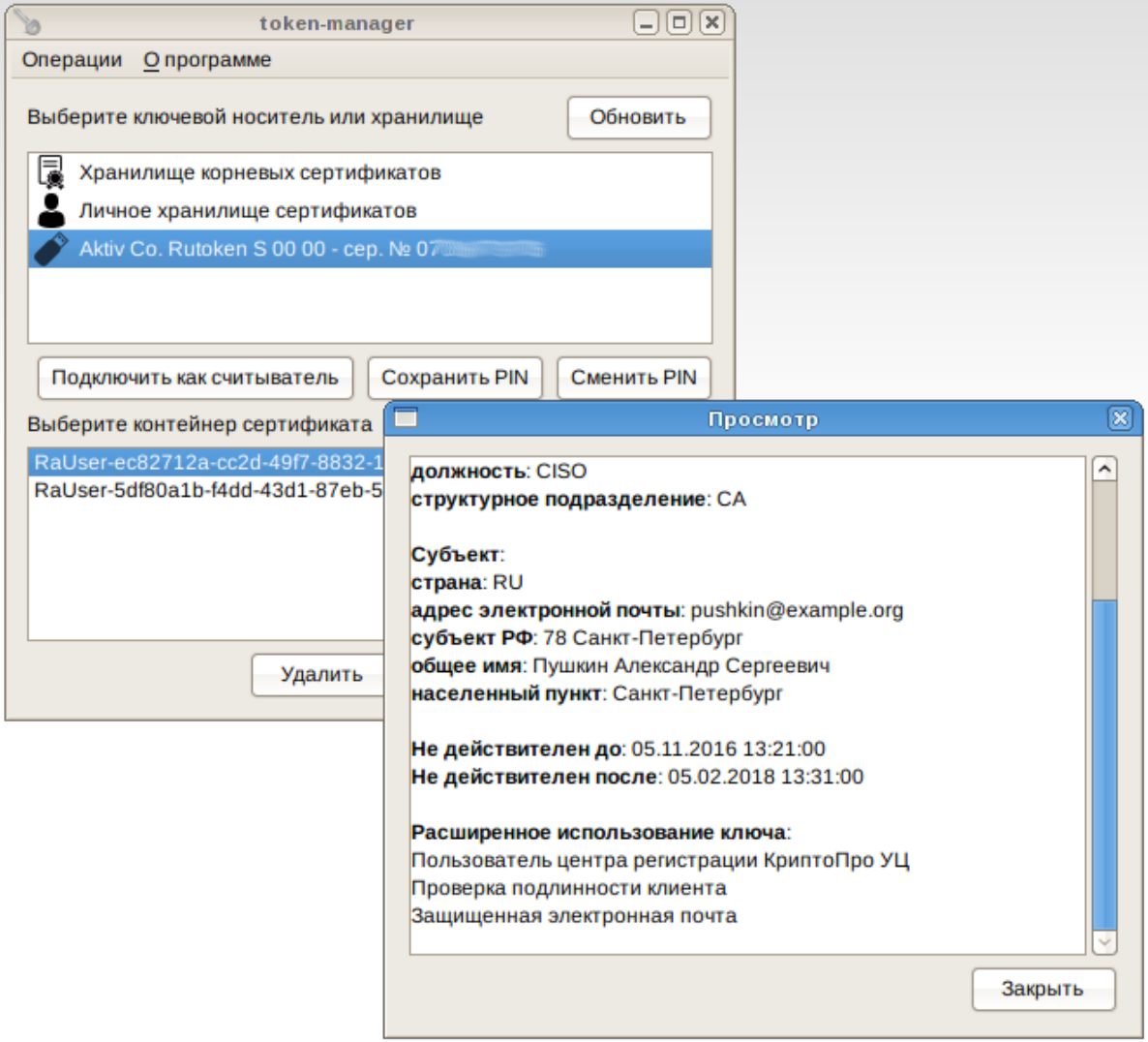
token-manager

Схема взаимодействия с КриптоПро CSP



token-manager

Как это выглядит?



gost-crypto-gui

Интегрированное в рабочее окружение
пользователя средство электронной подписи и шифрования файлов

gost-crypto-gui

В чем была проблема?

```
$ /opt/cprocsp/bin/amd64/cryptcp -sign -dn 'Чапаев Василий Иванович' Важный\ файл.txt
Certificate chains are checked.
Folder './':
list_pcsc... Signing the data...  0%CryptoPro CSP: Type pin-code for container
"RaUser-0f690419-c66c-4f90-ab2d-afd99c154537"
Pin-code:
Signed message is created.
[ReturnCode: 0]



$ /opt/cprocsp/bin/amd64/cryptcp -verify -verall Важный\ файл.txt.sig
CryptCP 3.41 (c) "Crypto-Pro", 2002-2013.
Command prompt Utility for file signature and encryption.
Folder './':
w.srt.sig... Signature verifying...
Signer: Чапаев Василий Иванович, 22-я стрелковая дивизия, Рабоче-крестьянская Красная Армия,
Красноярск, 24 Красноярский край, RU, chapai@example.org
The certificate revocation status or one of the certificates in the certificate chain is unknown.
Do you want to use this certificate ([Y]es, [N]o, [C]ancel)?Y

 Signature's verified.
[ReturnCode: 0]
```

gost-crypto-gui

Возможности

- Подпись файлов
- Проверка подписи
- Шифрование
- Расшифровка
- Интеграция с файловым менеджером
- Совместимость с PKCS#7

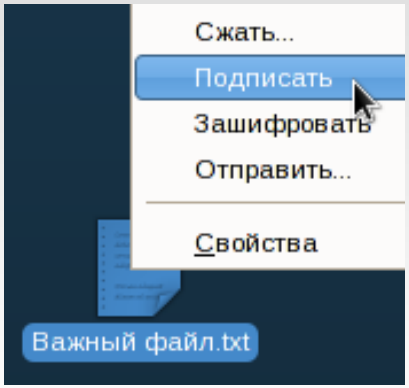
gost-crypto-gui

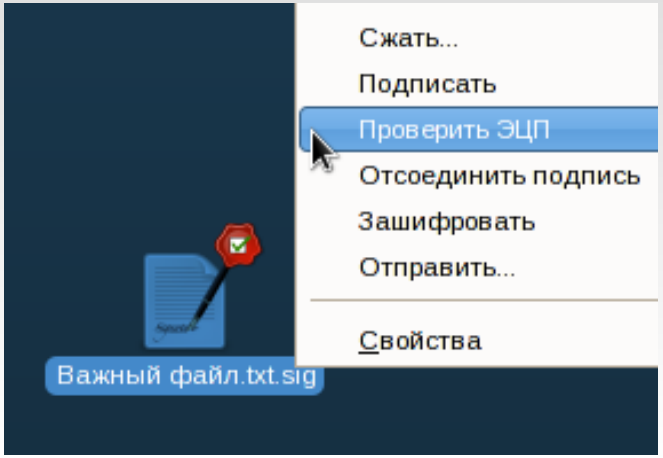
Дальнейшее развитие

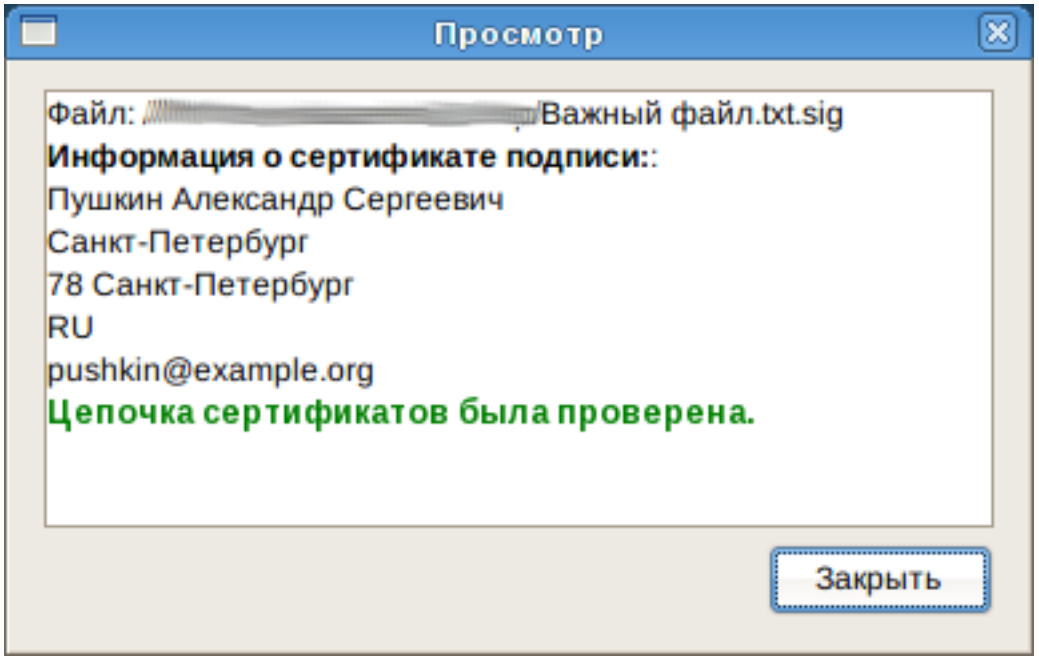
- Поддержка КриптоПро CSP 4.0
- Поддержка работы с отсоединённой подписью
- Использование меток времени
- Интеграция в окружения MATE и Cinnamon

gost-crypto-gui

Как это выглядит?







Заключение

Оба приложения распространяются по лицензии MIT. Вы можете свободно использовать их. В т.ч. включать в состав своих продуктов.

Установочные пакеты размещены в репозитории ОС «Гослинукс» и репозитории Sisyphus компании «Базальт СПО».

Разработка ведётся на GitHub.

makarenko@fssprus.ru

https://github.com/bmakarenko