

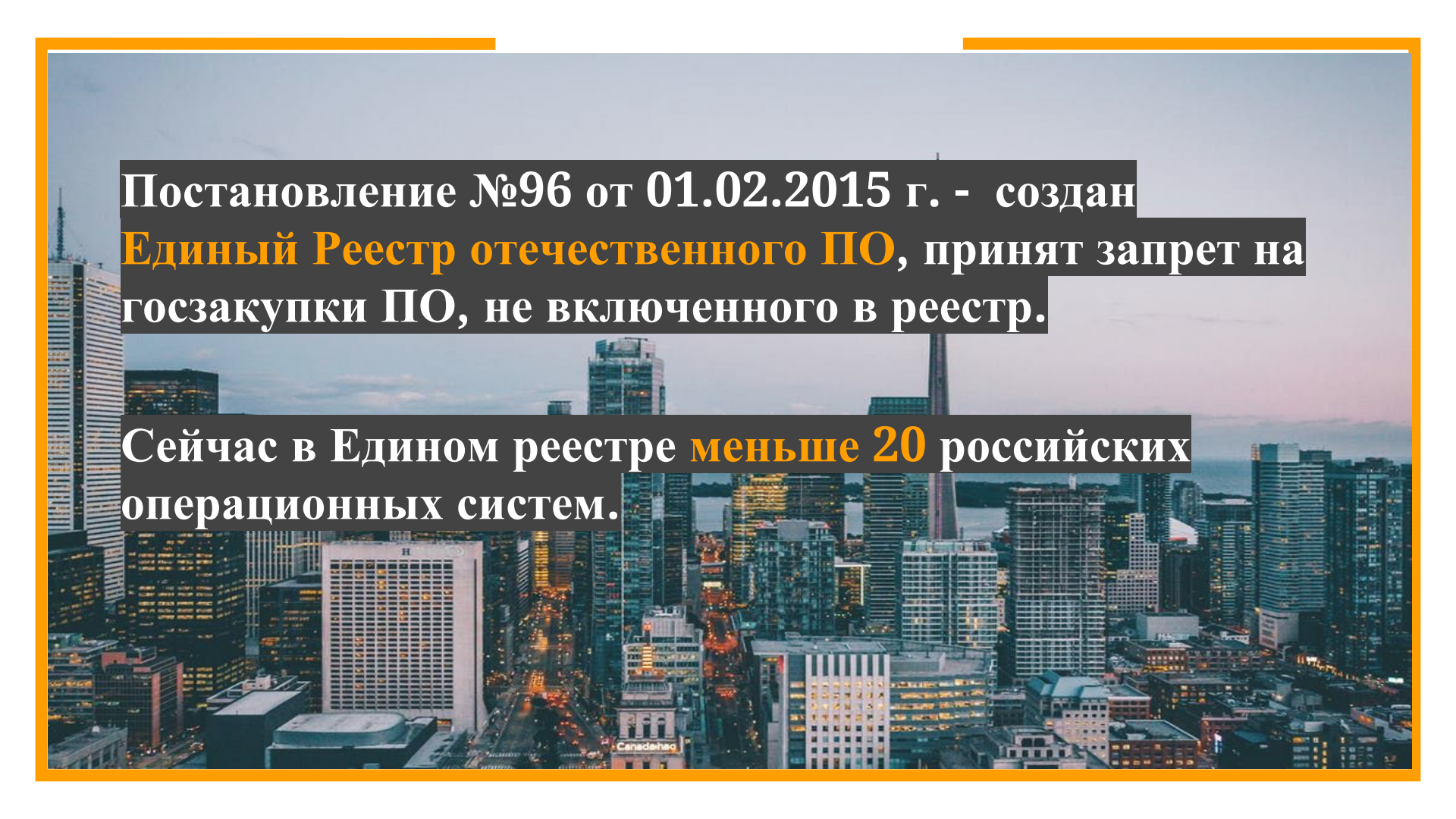
Конференция «ЮЗЭДО -
современный взгляд и
перспектива»



ПРИМЕНЕНИЕ СРЕДСТВ ЭЛЕКТРОННОЙ ПОДПИСИ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА ЛИНУКС

ООО «Цифровые технологии»
Андрей Селедкин

25 февраля 2018 г.

An aerial view of a city skyline at dusk, featuring numerous skyscrapers and buildings with illuminated windows. The sky is a mix of blue and orange. Two dark grey text boxes with white and orange text are overlaid on the image. The background image is framed by a thick orange border.

Постановление №96 от 01.02.2015 г. - создан
Единый Реестр отечественного ПО, принят запрет на
госзакупки ПО, не включенного в реестр.

Сейчас в Едином реестре **меньше 20** российских
операционных систем.

АЛТ БАЗАЛТ СПО

РОСА ИТЦ ИТ РОСА

ASTRA LINUX ИПО РУСБИТЕХ

РЕД РЕД СОФТ

Calculate Linux Альфа ОС

AlterOS Синергия Ульяновск.BSD



**Некоторые известные ОС не включены
в единый реестр**

ОС ГОСЛИНУКС **ФССП** **НЕТ В РЕЕСТРЕ**

ОС ОСЬ **РОСТЕХ** **НЕТ В РЕЕСТРЕ**

ПРИЧИНА: мало отличий от CentOS

Обычным пользователям для того
чтобы подписать электронный документ
с обеспечением условий для ЮЗЭДО

- квалифицированный сертификат
- сертифицированное СКЗИ
- интерфейс для подписи

ПРОГРАММНЫЕ СКЗИ на LINUX

**КриптоПро CSP VipNet CSP Крипто-КОМ
ЛИРССЛ-CSP**

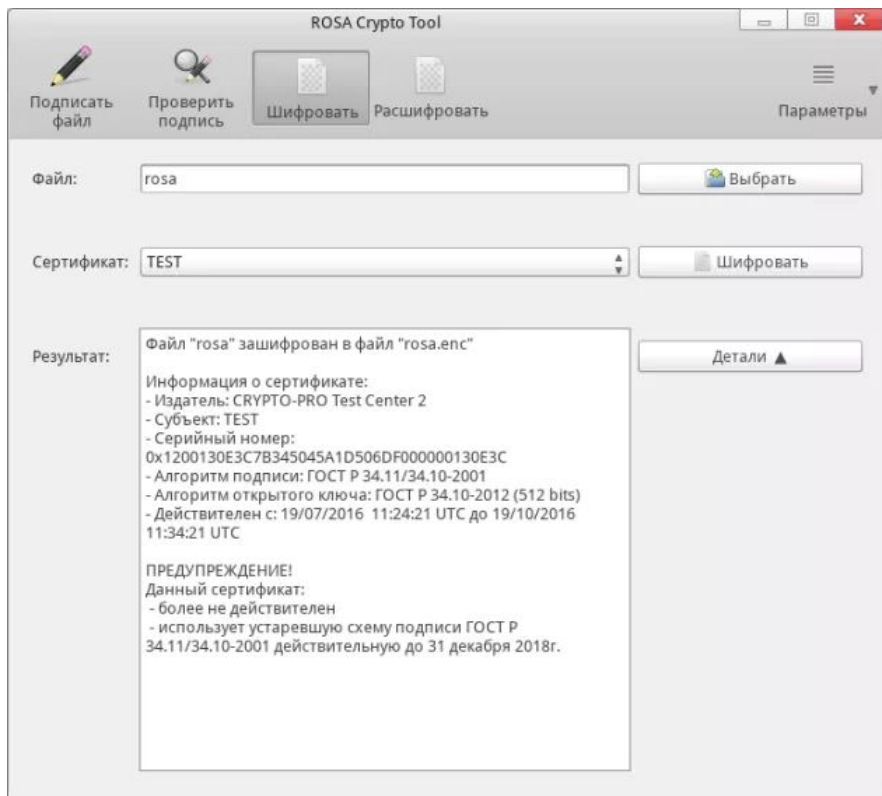
АППАРАТНЫЕ СКЗИ на LINUX

**Рутокен ЭЦП 2.0 JaCarta ГОСТ
eSmart Token ГОСТ MS_Key К Ангара**

**Зачем нужен
интерфейс?**

**Чтобы по
возможности
не использовать
консольные
команды**

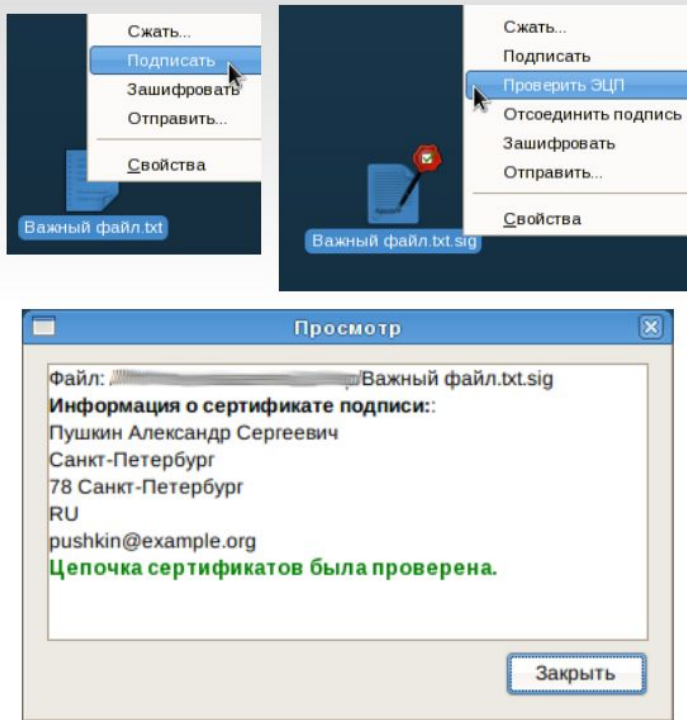
```
plx@plx:~/keybuild$ cat certificate.pem
-----BEGIN CERTIFICATE-----
MIIC9TCCAd2gAwIBAgIJAOG1y7946JwvMA0GCSqGSIb3DQEBCwUAMBExDzANBgNV
BAMMBm1pZGNhdD AeFw0xNjExMTUxNjM1NTJJaFw0xNzExMTAxNjM1NTJAMBExDzAN
BgNVBAMMBm1pZGNhdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL8g
s2Qj5LKvJNkRGh4Y+hCQwKtcz4Jk+sPWCi6IMLHEqaZes+bPehPedOPNN35PtN4b
n4Mbq2a9LjAvroCTLZm8cLdyMrUUtYPjrbVIm/x3tY/7A//QGb9dAx5r2+ILbM1F
HYoDfn0AE40uCzDrUSMbQHAHJshrbRIDeNVw4dHIeWdph7DmE91vBHayfp5IZshj
9/ARkn3ZurSoqkxkNfE/EHfwi9H1MoCve2Vp09+vNgSj10NsEK5MYdpTXyxxwRjc
a9HI6zqi6DwbTnUKql34wj90S4r2Ln75bgdRgvv0G2kdL1mVNB3+l/7A94LO/5uK
DkIR+bmuJMTml6nmHyECAwEAAaNQME4wHQYDVIR00BBYEF0A7JPgCNqCUqy7YRWOC
rqp8nZ02MB8GA1UdIwQYMBaAFOA7JPgCNqCUqy7YRWOCrqp8nZ02MAwGA1UdEwQF
MAMBAF8wDQYJKoZIhvcNAQELBQADggEBAIc3t5PjBw7cKhmtqBaNwpV5LxwFkaES
q6pA+KZVHdkZACSCg3RqFoto8q8k0GnYh0p01fJnY26dKhawcHkF1/VrL9cNq4tg
JxFA3vdi/fthoMTXEZJP7Jg6Ij36wjweQ51gI4ZMjrgFW9/QWqdjEmXH83Fe3Z2a
nJpndaPMOxAg8QsgS4Ce09a2gjlRk/WaIGQCXAjJb1Fcp3DNuFKAmYBCL9Etp8b3
h0IuY0dXnN0igft/FKwiAtJW8VERXkzuUoGDjUv4obJALeNVLG0Pa/uu1GHN3J73
MnBM4GnuH30px5Z3hygaq2+bPsK43x/9Uj1zhe+D0tIdASE7EQmo/GU=
-----END CERTIFICATE-----
plx@plx:~/keybuild$
```



ROSA CRYPTO TOOL

- ▣ Подпись
- ▣ Проверка подписи
- ▣ Шифрование
- ▣ Расшифрование
- ▣ КриптоПро CSP
- ▣ Рутокен
- ▣ ГОСТ 2012

<https://www.rosalinux.ru/2016/1/01/rosa-crypto-tool/>



gost-crypto-gui

- Подпись
- Проверка подписи
- Шифрование
- Расшифрование
- Сертификаты
- КриптоПро CSP
- Token manager
- Nautilus, Caja

<https://github.com/bmakarenko/gost-crypto-gui>

КриптоАРМ ГОСТ

- Подпись
- Проверка
- Шифрование
- Расшифрование
- Сертификаты
- Подкл. токенов

КриптоАРМ ГОСТ RU

Приложение КриптоАРМ ГОСТ предназначено для создания электронной подписи и шифрования файлов с применением цифровых сертификатов и криптографических алгоритмов

ЭЛЕКТРОННАЯ ПОДПИСЬ
Операции с электронной подписью для любых типов документов и произвольного контента

ШИФРОВАНИЕ ДАННЫХ
Защита пакетов документов и произвольного контента с помощью шифрования в адрес одного или нескольких получателей

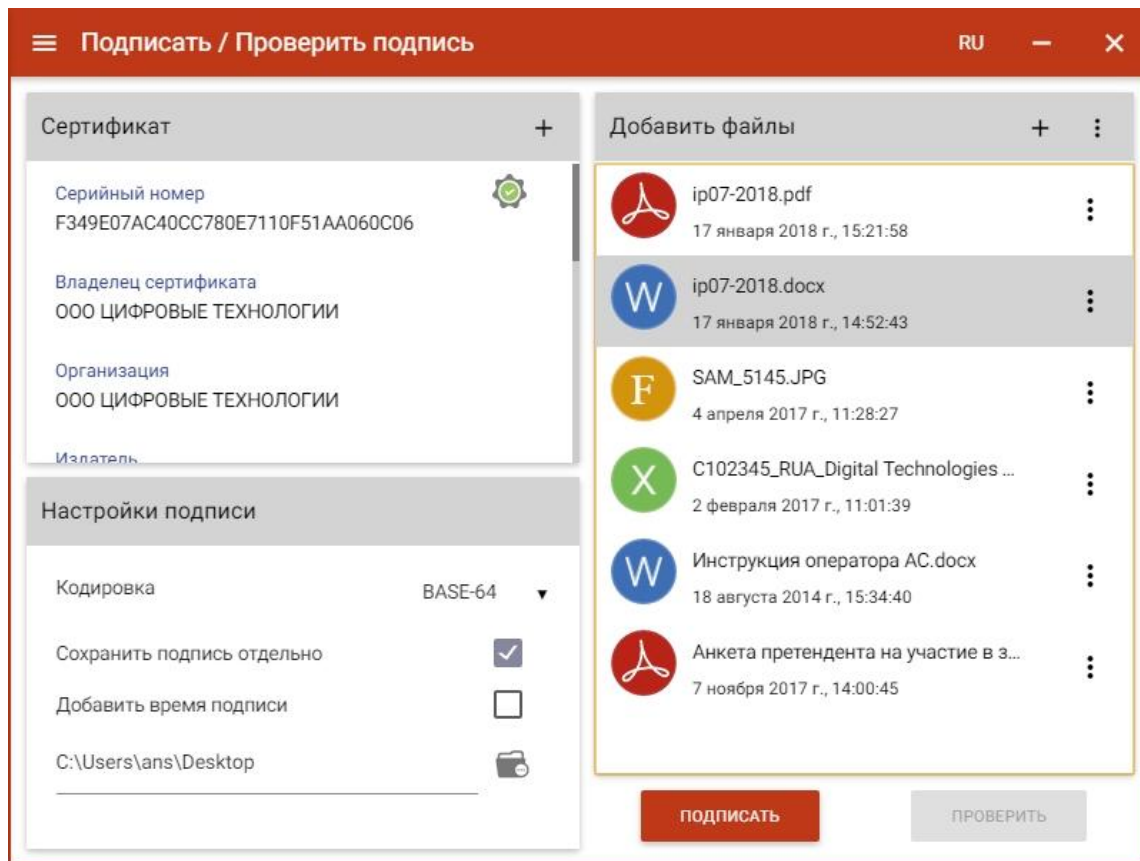
УПРАВЛЕНИЕ СЕРТИФИКАТАМИ
Централизованное управление локальными и облачными хранилищами сертификатов

ЦТ ООО Цифровые технологии
Copyright 2016-2017

КриптоАРМ ГОСТ

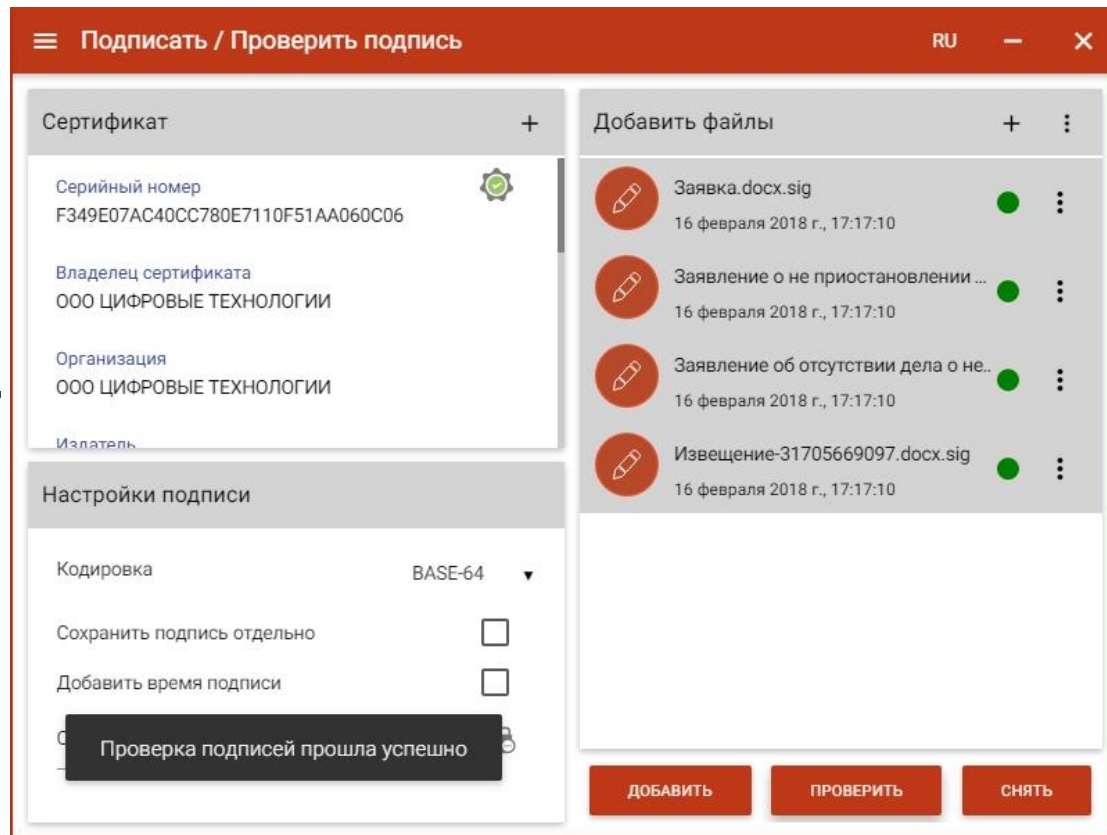
- Интерфейс на Electron
- Поддержка drag & drop
- Единые окна

<https://www.cryptoarm.ru/shop/cryptoarm-gost>



КриптоАРМ ГОСТ

- Совместимость с КриптоПро
- Поддержка usb-токенов
- Поддержка российских Линукс





Trusted eSign

Приложение для подписи и шифрования файлов на ОС семейства Linux и macOS

Создано на **Trusted API**
GUI для Trusted eSign

<https://github.com/TrustedPlus/esign>

Сайт FREE version

<https://trustedplus.github.io/>



OpenSSL

TRUSTED API

trusted-crypto

build passing coverage 84%

- CMS
- PKI
- XML Crypto
- PKCS#11



ELECTRON

Спасибо за внимание!

+7 (8362) 33-70-50

andrey.selyodkin@dig.t.ru

Андрей Селедкин, ООО «Цифровые технологии»,