python-pyopenssl python2-pyopenssl perl-net-ssleay lua-sec lua52-sec lua51-sec haskell-hsopenssl haskell-openssl-streams

gcr

curl https://structure.mil.ru/download/doc/morf/military/files/crl\_20.crl|sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mca -stdin -crl

curl https://structure.mil.ru/download/doc/morf/military/files/ca2019.cer|sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mca -stdin

curl https://structure.mil.ru/download/doc/morf/military/files/ca2020.cer|sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mRoot -stdin

wget -q -O - https://www.cryptopro.ru/sites/default/files/products/csp/cryptopro\_key.pub > cryptopro\_key.pub

wget -q -O - https://www.cryptopro.ru/sites/default/files/products/csp/cryptopro\_key.pub | apt-key add -

"ssl" "OpenSSL library" "cprocsp-cpopenssl-base cprocsp-cpopenssl cprocsp-cpopenssl-gost"

"cprocsp-stunnel" "stunnel, SSL/TLS tunnel with GOST support"

"rdr" "cprocsp-rdr-pcsc cprocsp-rdr-emv cprocsp-rdr-inpaspot cprocsp-rdr-mskey cprocsp-rdr-novacard cprocsp-rdr-rutoken"

Create HDIMAGE on root:

/opt/cprocsp/sbin/amd64/cpconfig -hardware reader -add HDIMAGE store

chmod 700 /var/opt/cprocsp/keys/username/newkeys.000

chmod 600 /var/opt/cprocsp/keys/username/newkeys.000/\*

chown -R username:username /var/opt/cprocsp/keys/username/newkeys.000

/opt/cprocsp/bin/amd64/csptest -keyset -enum\_cont -fqcn -verifyc

/opt/cprocsp/bin/amd64/csptest -keyset -check -cont '\\.\HDIMAGE\newkeys\_KEY\_FOR\_USER'

/opt/cprocsp/bin/amd64/certmgr -inst -store uMy -file newkeys.crt -cont \\.\HDIMAGE\newkeys\_KEY\_FOR\_USER'

/opt/cprocsp/bin/amd64/certmgr -list

GOSUSLUGI

lsb-cprocsp-pkcs11 cprocsp-rdr-gui-gtk

(IFCPlugin)

x86:

sudo cp ~/ifcx86.cfg /etc/ifc.cfg

/opt/cprocsp/bin/ia32/csptestf -absorb -certs -autoprov

x64:

sudo cp ~/ifcx64.cfg /etc/ifc.cfg

/opt/cprocsp/bin/amd64/csptestf -absorb -certs -autoprov

For chromium to comand:

sudo cp /etc/opt/chrome/native-messaging-hosts/ru.rtlabs.ifcplugin.json /etc/chromium/native-messaging-hosts

Extension:

https://chrome.google.com/webstore/detail/ifcplugin-extension/pbefkdcndngodfeigfdgiodgnmbgcfha

/opt/cprocsp/bin/amd64/csptestf -tlsc -server zakupki.gov.ru -v -nosave -savecert /tmp/t.p7b

/opt/cprocsp/bin/amd64/certmgr -list -file /tmp/t.p7b

/opt/cprocsp/bin/amd64/csptest -keyset -verifycontext

sudo /opt/cprocsp/sbin/amd64/cpconfig -ini '\config\parameters' -add long Rfc6125\_NotStrict\_ServerName\_Check 1

sudo /opt/cprocsp/bin/amd64/csptestf -tlsc -server zakupki.gov.ru -nosave

sudo /opt/cprocsp/sbin/amd64/cpconfig -ini '\config\parameters' -add bool Rfc6125\_NotStrict\_ServerName\_Check true

sudo /opt/cprocsp/bin/amd64/csptestf -tlsc -server zakupki.gov.ru -nosave

/etc/ifc.cfg

{ name = "CryptoPro CSP5";

alias = "cprocsp5";

type = "pkcs11";

alg = "gost2001";

model = "CPPKCS 3";

lib\_linux = "/opt/cprocsp/lib/amd64/libcppkcs11.so";

},

{ name = "CryptoPro CSP5 2012 256";

alias = "cprocsp5\_2012\_256";

type = "pkcs11";

alg = "gost2012\_256";

model = "CPPKCS 3";

lib\_linux = "/opt/cprocsp/lib/amd64/libcppkcs11.so";

},

{ name = "CryptoPro CSP5 2012 512";

alias = "cprocsp5\_2012\_512";

type = "pkcs11";

alg = "gost2012\_512";

model = "CPPKCS 3";

lib\_linux = "/opt/cprocsp/lib/amd64/libcppkcs11.so";

}

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

Chromium-Gost

makepkg -sCc --skipchecksums --noconfirm --skippgpcheck

/opt/cprocsp/sbin/amd64/cpconfig -license -view

/opt/cprocsp/sbin/amd64/cpconfig -license -set CODE

/opt/cprocsp/bin/amd64/csptest -card -enum -v -v

/opt/cprocsp/bin/amd64/csptest -keyset -enum\_cont -fqcn -verifyc

/opt/cprocsp/bin/amd64/csptestf -absorb -cert

/opt/cprocsp/bin/amd64/certmgr -list -store uMy

Импорт коренвых сертификатов в хранилище доверенных корневых сертификатов

sudo /opt/cprocsp/bin/amd64/certmgr -inst -store uroot -file "uc\_tensor\_44-2017.cer"

sudo /opt/cprocsp/bin/amd64/certmgr -inst -store uroot -file "uc\_tensor-2018\_gost2012.cer"

sudo /opt/cprocsp/bin/amd64/certmgr -inst -store uroot -file "uc\_tensor-2017.cer"

Установка всех личных сертификатов со всех контейнеров в uMy :

$ /opt/cprocsp/bin/amd64/csptestf -absorb -certs -autoprov

Установка определенного сертификата с определенного контейнера в uMy:

$ /opt/cprocsp/bin/amd64/certmgr -inst -cont '\\.\Aktiv Rutoken ECP 00 00\Ivanov'

Установка сертификата удостоверяющего центра ГУЦ в mRoot:

$ sudo curl https://structure.mil.ru/download/doc/morf/military/files/ca2020.cer|sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mRoot -stdin

Установка промежуточного сертификата МО в mca:

$ sudo curl https://structure.mil.ru/download/doc/morf/military/files/ca2019.cer|sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mca -stdin

Установка списка отвызвов (CRL), ставим его с того же сайта в mca:

$ sudo curl https://structure.mil.ru/download/doc/morf/military/files/crl\_20.crl|sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mca -stdin -crl

Удаление контейнера

Для удаления контейнера следует воспользоваться командой:

/opt/cprocsp/bin/amd64/csptestf -passwd -cont '\\.\Aktiv Rutoken ECP 00 00\TestCont' -deletek

Копирование контейнера

Для примера скопируем контейнер из локального хранилища в хранилище Рутокена ЕЦП:

csptestf -keycopy -contsrc '\\.\HDIMAGE\Контейнер\_оригинал' -contdest '\\.\Aktiv Rutoken ECP 00 00\Контейнер\_копия'

Удаление

Удаление сертификата из хранилища КриптоПро:

certmgr -delete 1 (номер сертификата)

certmgr -del -all (удаление всех сертификатов)

Экспорт самих сертификатов (если их 14):

for i in `seq 1 14`; do echo $i | certmgr -export -dest $i.cer; done

Переносим эти файлы на машину и смотрим, какие контейнеры есть:

csptest -keyset -enum\_cont -verifycontext -fqcn

И как обычно, связываем сертификат и закрытый ключ:

certmgr -inst -file 1.cer -cont '\\.\HDIMAGE\container.name'

Test Browser Plugin

https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades\_bes\_sample.html

/opt/cprocsp/bin/amd64/certmgr -list -store root

/opt/cprocsp/bin/amd64/certmgr -list -store CA

/opt/cprocsp/bin/amd64/certmgr -list -store My

Назначение хранилищ:

Есть три хранилища. по умолчанию: CA, ROOT, My[1].

CA для списков СОС и промежуточных центров сертификации,

ROOT для сертификатов корневых центров сертификации и

My для личных сертификатов.

Имя хранилища является регистронезависимым.