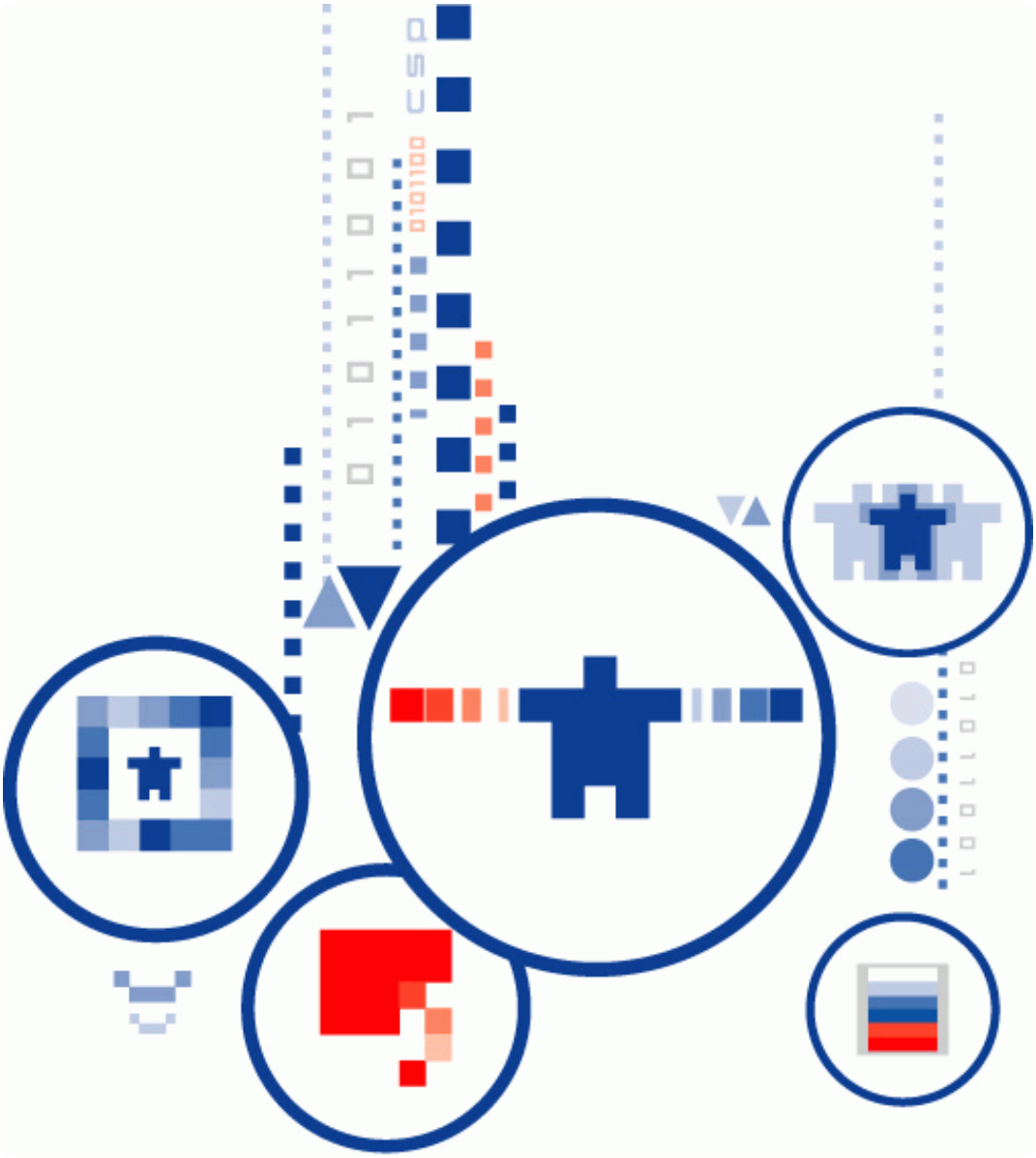

КриптоПро PKI-Кластер
Сервис проверок

Руководство администратора

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

CSP	—	Криптопровайдер (Cryptographic Service Provider)
SSL	—	Протокол защиты сокетов (Secure Sockets Layer)
TLS	—	Протокол защиты транспортного уровня (Transport Layer Security)
URL	—	Единый указатель ресурсов (Uniform Resource Locator)
АПМЗ	—	Аппаратный модуль доверенной загрузки
БД	—	База данных
ЗПС	—	Замкнутая программная среда
ИС	—	Информационная система
НСД	—	Несанкционированный доступ
СУБД	—	Система управления базой данных
ОС	—	Операционная система
ПО	—	Программное обеспечение
СЗИ	—	Средство защиты информации
СКЗИ	—	Средство криптографической защиты информации
ЭП	—	Электронная подпись
ПАК	—	Программно-аппаратный комплекс
УЦ	—	Удостоверяющий Центр

СОДЕРЖАНИЕ

1. Аннотация

Настоящий документ содержит Руководство администратора Сервиса проверок ПК «КриптоПро PKI-Кластер» (далее – Сервиса проверок).

Документ включает в себя сведения описание процесса разворачивания и настройки основных технических и программных решений и предназначен для системных администраторов и Администраторов PKI-Кластер как руководство по установке и конфигурированию PKI-Кластер.

2. Системные требования

2.1. Требования к аппаратному обеспечению

Аппаратные требования к техническим средствам, на которых размещаются программные компоненты Сервиса проверок, зависят от требований по производительности всего комплекса.

Таблица 1. Требования к аппаратному обеспечению

Оборудование	Минимальные требования
Центральный процессор	64-разрядный двухъядерный процессор с тактовой частотой 1,86 ГГц
Оперативная память	4 ГБ ОЗУ
Жесткий диск	4 ГБ свободного места
Сетевые адаптеры	Один сетевой адаптер, совместимый с операционной системой компьютера, для взаимодействия с внутренней сетью
СЗИ от НСД	АПМЗ в соответствии с эксплуатационной документацией на СКЗИ

2.2. Требования к программному обеспечению

В Таблица 2 указаны предъявляемые к программному обеспечению требования.

Таблица 2. Требования к программному обеспечению

Компонент	Наименование
Операционная система	Astra Linux Special Edition в режиме ЗПС
СУБД	PostgreSQL
Веб-сервер	➢ Nginx с патчем ng-nginx.1.18.0.patch, ➢ Apache с модулем СКЗИ. Применение допустимо в соответствии с эксплуатационной документацией на СКЗИ
Антивирусное ПО	В соответствии с эксплуатационной документацией на СКЗИ
СКЗИ	КриптоПро CSP 5.0 R2

3. Развертывание Сервиса проверок

В данном разделе описывается развертывание Сервиса проверок. Для выполнения развертывания Сервиса проверок необходимо выполнить следующие шаги:

1. Установка ОС.
2. Установка КриптоПро CSP.
3. Установка веб-сервера.
4. Установка СУБД.
5. Установка ПО Сервиса проверок и дополнительного ПО.

3.1. Установка ОС

Дистрибутив Astra Linux Special Edition необходимо получить самостоятельно. Установка выполняется согласно эксплуатационной документации на ОС СН Astra Linux SE Смоленск.

Для отображения печатных форм в Сервисе проверок необходимо установить пакет **libgdiplus**.

Для обеспечения взаимодействия с АИС Налог необходимо установить пакет **gss-ntlm**

3.2. Установка КриптоПро CSP

Дистрибутив необходимо получить самостоятельно. Установка выполняется согласно эксплуатационной документации на КриптоПро CSP 5.0 КС3.

3.3. Развертывание веб-сервера

Необходимо выполнить настройку веб-серверов nginx или Apache согласно эксплуатационной документации на КриптоПро CSP 5.0 КС3.

3.3.1. Пример развертывания и настройки веб-сервера nginx

Для настройки работы веб-сервера необходимо установить **nginx с патчем ng-nginx.1.18.0.patch** из состава дистрибутива КриптоПро CSP.

ППО nginx не входит в комплект поставки СКЗИ. Исходные тексты nginx 1.18.0 скачиваются с официального сайта с последующей проверкой контрольной суммы, указанной в документации на СКЗИ.

После применения патча осуществляется сборка «пропатченных» исходных текстов сервера nginx с последующим вычислением ЭП (в соответствии с эксплуатационной документацией на ОС Astra Linux SE) для возможности их использования в замкнутой программной среде (ЗПС) ОС Astra Linux SE.

Перед установкой nginx на сервер необходимо загрузить патч ng-nginx.1.18.0. patch и init-скрипт nginx.init.

Пример разворачивания веб-сервера nginx

- Установка дополнительных пакетов:

```
sudo apt-get install build-essential patch
```

- Применение модуля СКЗИ для nginx:

```
wget https://nginx.org/download/nginx-1.18.0.tar.gz
tar -xvf ./nginx-1.18.0.tar.gz
cp ./ng-nginx.1.18.0.patch ./nginx-1.18.0 && cd ./nginx-1.18.0/
patch -p1 < ./ng-nginx.1.18.0.patch
```

- Получение дополнительных исходных текстов:

```
wget https://ftp.pcre.org/pub/pcre/pcre-8.44.tar.gz
tar -xvf ./pcre-8.44.tar.gz && cd ./pcre-8.44
wget https://zlib.net/zlib-1.2.11.tar.gz
tar -xvf ./zlib-1.2.11.tar.gz
wget https://www.openssl.org/source/openssl-1.1.1h.tar.gz
tar -xvf ./openssl-1.1.1h.tar.gz
```

- Сборка:

```
cd ./nginx-1.18.0
./configure \
--user=nginx \
--group=nginx \
--with-cc-opt='-fstack-protector -fstack-protector-strong --param=ssp-buffer-
size=4 -Wformat -Werror=format-security -Werror=implicit-function-declaration
-Winit-self -Wp,-D_FORTIFY_SOURCE=2 -fPIC' \
--with-ld-opt='-Wl,-z,relro -Wl,-z,now -Wl,--as-needed -pie -
L/opt/cprocsp/lib/amd64 -lrdrsup -lssp -lcapi10 -lcapi20' \
--prefix=/opt/nginx \
--conf-path=/etc/nginx/nginx.conf \
--error-log-path=/var/log/nginx/error.log \
--http-log-path=/var/log/nginx/access.log \
--lock-path=/var/run/lock/nginx.lock \
--pid-path=/var/run/nginx.pid \
--with-pcre=/home/test/src/pcre-8.44/ \
--with-pcre-jit \
--with-zlib=/home/test/src/zlib-1.2.11/ \
--with-http_ssl_module \
--with-http_sspi_module \
--with-http_stub_status_module \
--with-openssl=/home/test/src/openssl-1.1.1h/ \
--with-openssl-opt='no-gost no-comp no-dtls no-deprecated no-dynamic-engine
no-engine no-hw-padlock no-nextprotoneg no-psk no-tests no-ts no-ui-console'
\
--with-stream \
--with-stream_ssl_module \
--with-stream_sspi_module \
--with-http_v2_module
```

- Запуск сборки:

```
make
```

- Копирование базовой конфигурации (пример конфигурации приведён в 3.3.3):

```
sudo cp ./nginx.conf.sample ./nginx-1.18.0/conf/nginx.conf
```

```
sudo make install
```

- Создание системного пользователя:

```
sudo adduser --system --no-create-home --group nginx
sudo chown -R nginx:nginx /var/log/nginx/
```

- Перенос init-скрипта:

```
sudo cp ./nginx.init /etc/init.d/nginx
```

3.3.2. Работа с ключами и сертификатами

В рамках задач Сервиса проверок для nginx необходимо подготовить сертификат веб-сервера TLS. Требования к нему такие же, как к серверным сертификатам - наличие в субъекте или расширении "Дополнительное имя субъекта" (SAN) имени хоста и наличие Проверка подлинности сервера (1.3.6.1.5.5.7.3.1) в расширении "Улучшенный ключ". Ниже описан пример установки сертификата из pfx. В этом варианте, сертификат веб-сервера должен быть получен заранее на ЦС и скопирован на сервер с компонентами Сервиса проверок в виде pfx файла.

```
sudo -u nginx /opt/cprocsp/bin/amd64/certmgr -install -pfx -store uMy -file
/<path>/certificate.pfx -pin <пароль от файла pfx>
```

Для успешной проверки серверных и клиентских сертификатов необходимо установить сертификаты всех вышестоящих УЦ. Ниже пример установки корневых и промежуточных сертификатов УЦ. (где uRoot – хранилище корневых сертификатов, uCa – хранилище промежуточных сертификатов)

```
sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mRoot -file /<path>/root.cer
sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mCa -file /<path>/to/ca.cer
```

3.3.3. Конфигурация nginx для Сервиса проверок

Для обеспечения работоспособности Сервиса проверок nginx необходимо настроить в режимах двусторонней аутентификации по сертификату (Mutual TLS) и обратного прокси-сервера (reverse-proxy). Ниже приведен пример конфигурации nginx.

```
server {
 listen 443;
 server_name ecpserver; # DNS – имя сервера ЕЦП
 proxy_set_header Host $host;
 proxy_set_header X-Real-IP $remote_addr;
 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 proxy_set_header X-Forwarded-Proto $scheme;
 proxy_set_header X-SSL-CERT $sspi_client_escaped_cert;

 # ECP Web
 location / {
 proxy_pass http://localhost:5000;
 proxy_buffer_size 64k;
 proxy_buffers 4 64k;
 proxy_busy_buffers_size 64k;
 }
 # ECP API
 location /api/smev {
 proxy_pass http://localhost:5000;
 }
 sspi on;
```

```
 sspi_certificate 0x4ACAE00070AC82A84C2660BBDC1DD3A1; # Серийный номер
сертификата веб-сервера
 sspi_protocols TLSv1 TLSv1.1 TLSv1.2;
 sspi_verify_client on;
 sspi_client_certificate root;
 }
```

После изменения конфигурации nginx необходимо перезапустить:

```
sudo systemctl stop nginx && sudo systemctl start nginx
```

3.4. Установка СУБД

Установка и настройка выполняется согласно эксплуатационной документации на СУБД PostgreSQL. Ниже указан пример установки.

```
sudo apt-get install postgresql
```

3.5. Установка ПО Сервиса проверок

3.5.1. Подготовка дистрибутива Сервиса проверок

Дистрибутив Сервиса проверок необходимо скопировать на сервер в директорию /opt/ecp/version_ecp/ (**допустимо указание другого пути**) и выдать права на исполнение следующим файлам:

```
chmod u+x
"/opt/ecp/version_ecp/CryptoPro.SmevArchive.Service/CryptoPro.SmevArchive.Ser
vice"
chmod u+x
"/opt/ecp/version_ecp/CryptoPro.SmevArchive.Web/CryptoPro.SmevArchive.Web"
chmod u+x "/opt/ecp/version_ecp/pkica/pkica"
chmod u+x "/opt/ecp/version_ecp/pkica-test/pkica-test"
```

Компонент nats-streaming необходимо скопировать в директорию /opt/ecp/ (**допустимо указание другого пути**).

```
chmod u+x "/opt/ecp/nats-streaming/nats-streaming-server"
```

В директории каждого приложения располагается конфигурационный файл **appsettings.json**. Для каждого приложения в файле **appsettings.json** необходимо указать путь (path) для сохранения логов приложений. Ниже указан пример для приложения CryptoPro.SmevArchive.Service.

```
"path": "/opt/ecp/log/CryptoPro.SmevArchive.Service_.log",
```

3.5.2. Развертывание базы данных Сервиса проверок

Для разворачивания СУБД Сервиса проверок необходимо выполнить следующие команды.

```
cd "/opt/ecp/version_ecp/pkica"
./pkica smev db new
```

3.5.3. Подготовка сервисных сертификатов

Для обеспечения функционирования Сервиса проверок необходимо подготовить следующие сервисные сертификаты:

1. Сертификат веб-сервера (см. 3.3.2).
2. Сертификат NATS Streaming (см. 6.1).
3. Сертификат Сервиса проверок (см. 6.2).
4. Сертификат веб-сервиса Сервиса проверок (см. 6.2).
5. Сертификат(-ы) Администратора.

3.5.4. Запуск сервиса NATS Streaming

Для запуска сервиса NATS Streaming необходимо:

- указать каталог хранения сообщений - параметр dir в файле конфигурации **nats.conf**, например:

```
/opt/ecp/nats-streaming/nats.conf;
```

- запустить сервис nats-streaming, выполнив следующую команду:

```
cd /opt/ecp/nats-streaming/ && ./nats-streaming-server -sc nats.conf
```

3.5.5. Запуск Сервиса проверок

Для запуска Сервиса проверок в файле **appsettings.json** приложения CryptoPro.SmevArchive.Service необходимо:

- указать параметры подключения к БД SmevArchive.Database:

```
"Database": {
"StorageType": "PostgreSql",
"ConnectionString":"Server=localhost;Database=
SmevArchive.Database;Username=postgres;Pooling=True"
```

- выполнить следующую команду:

```
cd /opt/ecp/version_ecp/CryptoPro.SmevArchive.Service &&
./CryptoPro.SmevArchive.Service
```

3.5.6. Запуск веб-сервиса Сервиса проверок

Для запуска веб-сервиса Сервиса проверок в файле **appsettings.json** приложения CryptoPro.SmevArchive.Web необходимо:

- указать параметры подключения к БД SmevArchive.Database:

```
"Database": {
"StorageType": "PostgreSql",
"ConnectionString":"Server=localhost;Database=
SmevArchive.Database;Username=postgres;Pooling=True"
```

- выполнить следующую команду:

```
cd /opt/ecp/version_ecp/CryptoPro.SmevArchive.Web &&
./CryptoPro.SmevArchive.Web
```

4. Настройка Сервиса проверок

4.1. Регистрация сервисов

В разделе ниже описан процесс создания юнитов в systemd для сервисов для обеспечения их автоматического управления Сервисом проверок.

Для этого необходимо выполнить следующие действия.

- Создать для каждого сервиса файл в следующей директории:

```
/etc/systemd/system/<имя сервиса>.service
```

- Применить изменения:

```
sudo systemctl daemon-reload
```

- Разрешить автозагрузку:

```
sudo systemctl enable <имя юнит-сервиса>
```

- Запустить сервис:

```
sudo systemctl start <имя юнит-сервиса>
```

- Пример файла <имя сервиса>:

```
[Unit]
Description=nats-streaming-server
[Service]
WorkingDirectory=/opt/ecp/nats-streaming
ExecStart=/opt/ecp/nats-streaming/nats-streaming-server -sc /opt/ecp/nats-
streaming/nats.conf
Restart=always
# Restart service after 10 seconds if the dotnet service crashes:
RestartSec=10
KillSignal=SIGINT
SyslogIdentifier=nats-streaming-server
User=cp
[Install]
WantedBy=multi-user.target
```

- Посмотреть информацию о работе сервисов можно при помощи следующих команд:

```
sudo systemctl status <имя приложения>
sudo journalctl -u <имя приложения>
```

4.2. Добавление Операторов Сервиса проверок

Для добавления Оператора Сервиса проверок с правами администратора необходимо выполнить команду:

```
./pkica smev operator add --last-name "Иванов" --first-name "Иван" --cert-
file /administrator.cer --group-name Administrators --is-admin
```

Для добавления оператора Ra.Service необходимо выполнить в терминале:

```
./pkica smev operator add --last-name "Петров" --first-name "Петр" --cert-
file /operator.cer --group-name Operator
```

4.3. Настройка взаимодействия с АИС Налог

Для обеспечения взаимодействия с АИС Налог в файле **appsettings.json** сервиса CryptoPro.SmevArchive.Service необходимо указать параметры подключения к АИС Налог. Ниже приведен пример конфигурации.

```
Url": "http://x.x.x.x:9400/inias/csc/gws/uc/ecpsvc/api/v1/", # адрес АИС
Налог
    "Credentials": {
    "UserName": "", # логин
    "Password": ""
```

Для проверки взаимодействия с АИС Налог в составе дистрибутива доступна утилита pkica-test

Выполнение команды ниже инициирует подачу запроса на проверку сведений о заявителе напрямую в ИС АИС Налог без участия PKI-Кластер.

```
./pkica-test ais-nalog check-cert-data -o "/home/new-user/ecp/pkica-test-
predefined-owners-fns-service/ais-nalog-ib.json" -u
"http://DNS/inias/csc/gws/uc/ecpsvc/api/v1/" --login "ЛОГИН" --password
"ПАРОЛЬ"
```

4.4. Настройка взаимодействия с СМЭВ

Для обеспечения взаимодействия с СМЭВ в файле **appsettings.json** сервиса CryptoPro.SmevArchive.Service необходимо указать параметры подключения к СМЭВ. Ниже приведен пример конфигурации.

```
"Url": " http://x.x.x.x:7500/smev/v1.2/ws?wsdl ", # адрес для подключения к
СМЭВ
"Thumbprint": "487bb29686ca84a4ddf8b36e2a49e6409f025934", # отпечаток
сертификата для подключения к СМЭВ
```

4.5. Эмуляция отправки запросов в СМЭВ

Для эмуляции отправки запросов в СМЭВ возможно использовать утилиту smevutil. При запуске с опцией PredefinedMessagesPath будет выдан список ИНН и СНИЛС для которых будут выполняться проверки.

```
Smevutil.exe -host -url http://localhost:9023/MessageExchange -thumbprint
f8a0a59e0d88bf5bda01a6eb4862a9149b25bbc9 -PredefinedMessagesPath "..\<папка с
additions файлами>\smevutil-predefined-messages\" -out -allget
```

- в папке smevutil-predefined-messages фалы для запуска smevutil для эмуляции СМЭВ по тестовым данным;
- в папке pkica-test-predefined-owners тестовые профили;

В случае, если переопределенных ответов недостаточно, то Smevutil можно запустить в режиме перенаправления запросов:

```
Smevutil.exe -host -url http://localhost:9023/MessageExchange -thumbprint
f8a0a59e0d88bf5bda01a6eb4862a9149b25bbc9 -PredefinedMessagesPath "..\<папка с
additions файлами>\smevutil-predefined-messages\" -redirectUrl
http://172.20.3.12:7500/smev/v1.2/ws?wsdl -out -allget
```

В режиме перенаправления запросов, smevutil буде перенаправлять запросы по адресу http://172.20.3.12:7500/smev/v1.2/ws?wsdl , в случае, если в папке smevutil-predefined-messages не будет найдено предопределенного ответа.

Для обеспечения взаимодействия с утилитой smevutil в фа*йле* ***appsettings.json*** *сервиса CryptoPro.SmevArchive.Service необходимо указать параметры* подключения к smevutil. Ниже приведен пример конфигурации.

```
"Url": "http://192.168.63.124:9023/MessageExchange", # адрес для подключения
к smevutil
"Thumbprint": "487bb29686ca84a4ddf8b36e2a49e6409f025934", # отпечаток
сертификата для подключения к smevutil
```

5. Обновление Сервиса проверок

Для обновления Сервиса проверок необходимо скопировать новый дистрибутив и выполнить поочередно следующие пункты:

1. Подготовка дистрибутива Сервис проверок (см. 3.5.1).

2. Остановить службы приложений предыдущей версии Сервиса проверок.

В случае изменения версии базы данных в новом дистрибутиве, необходимо выполнить следующие шаги:

1. Создать резервную копию БД Сервиса Проверок
2. Обновить версию БД используя новую версию утилиты командной строки pkica:

```
cd "/opt/ecp/new_version_ecp/pkica"
./pkica ra smev upgrade
```

3. Запустить службы приложений новой версии Сервиса проверок (см. 3.5.4-3.5.6).

6. Управление сервисными сертификатами

6.1. Пример назначения сертификата NATS Streaming

Для NATS Streaming необходим серверный сертификат. Требования к нему такие же, как к серверным сертификатам для веб-серверов - наличие в субъекте или расширении "Дополнительное имя субъекта" (SAN) имени хоста и наличие Проверка подлинности сервера (1.3.6.1.5.5.7.3.1) в расширении "Улучшенный ключ". Возможный способ выпуска такого сертификата - использование соответствующего мастера из Диспетчера УЦ 2.0. Действия по установке:

1. Выпустить серверный сертификат. Если серверный сертификат был выпущен сразу в формате PEM, то сразу перейти к шагу 4.
2. Выгрузить сертификат в pfx.
3. Сконвертировать полученный pfx в формат PEM с помощью утилиты openssl. Команды для конвертации:

```
openssl pkcs12 -in <сервер>.pfx  -nocerts -nodes -out <ключ сервера>.pem
openssl pkcs12 -in <сервер>.pfx  -nokeys -clcerts -out <сертификат
сервера>.pem
```

- Добавить путь к полученным файлам ключа и сертификата в файл конфигурации NATS в разделы **tls** и **streaming.tls.**

```
...
tls: {
# серверный сертификат NATS
  cert_file: "путь к <сертификат сервера>.pem"
  key_file:  "путь к <ключ сервера>.pem"
  verify_and_map: true
}
...
streaming: {
...
# сертификат NATS Streaming для подключения к сервису NATS
    tls: {
        client_cert: "путь к <сертификат сервера>.pem"
        client_key: "путь к <ключ сервера>.pem"
    }
}
```

Сертификаты необходимо установить в хранилище **umy** от имени пользователя, под которым будут запущены сервисы.

6.2. Пример назначения сервисных сертификатов Сервиса проверок

В Шлюзе прикладного уровня сервисы NATS используют CryptoPro.SmevArchive.Service и CryptoPro.SmevArchive.Web. Для всех них настройка защищенного подключения к NATS производится аналогичным образом, путем редактирования файла **appsettings.json**. Сертификат для подключения является обычным клиентским TLS сертификатом с Проверка подлинности клиента

(1.3.6.1.5.5.7.3.2) в расширении “Улучшенный ключ”, поэтому для его выпуска возможно использовать мастер выпуска клиентского сертификата ЦР из Диспетчера УЦ 2.0. Действия по настройке: 1. Выпустить клиентский сертификат. Так как для каждого компонента сертификат настраивается отдельно, то необходимо, чтобы сертификат содержал отличительный признак того, какой компонент этот сертификат будет использовать. Этим признаком может быть уникальной значение DNS имени или email в расширении “Дополнительное имя субъекта” (SAN), либо субъект сертификата целиком. 2. Если сертификат был получен в формате PEM, то сконвертировать его в PFX с помощью openssl:

```
openssl pkcs12 -inkey <ключ>.pem -in <сертификат>.pem -export -out
<сертификат>.pfx
```

- Установить сертификат в хранилище “Личное”. Для этого можно воспользоваться утилитой certmgr:

```
certmgr -install -store umy -file <файл сертификата>.cer -provtype 80 -
container <имя контейнера>
```

Сертификаты необходимо установить в хранилище **umy** от имени пользователя, под которым будут запущены сервисы.

- В конфигурационном файле **appsettings.json** компонента включить защищенное соединение "Secure": true и добавить отпечаток сертификата в существующие разделы Nats и Stan:

```
...
"Nats": {
  "Url": "nats://localhost:4222",
  "Secure": true,
  "Thumbprint": "<отпечаток клиентского сертификата>"
},
...
"Stan": {
  "Url": "nats://localhost:4222",
  ...
  "Secure": true,
  "Thumbprint": "<отпечаток клиентского сертификата>"
},
```

- В конфигурационном файле NATS Streaming добавить уникальный признак сертификата в раздел сопоставления authorization.users для соответствующего компонента. Если в качестве уникального признака используется субъект целиком, то в конфигурационный файл он прописывается в виде текстовой строки с компонентами, разделенными запятыми без пробелов. Порядок компонент обратный (как в окне просмотра сертификата). Если в субъекте есть повторяющиеся компоненты, то используется только первый. Пример для CryptoPro.SmevArchive.Web:

```
authorization: {
...
  users = [
  ...
     {user: "<уникальный признак сертификата>", permissions: $RA_WEB} #
сопоставление сертификата для CryptoPro.SmevArchive.Web
  ...
  ]
}
```

- После настройки защищенного соединения для всех компонентов для применения настроек необходимо перезапустить NATS Streaming.

7. Дополнительные настройки компонент Сервиса проверок

7.1. Настройки Сервиса проверок

Конфигурация (настройки) сервиса проверок определяются параметрами в файле appsettings.json приложения CryptoPro.SmevArchive.Service.

Таблица 3. Параметры приложения CryptoPro.SmevArchive.Service

Блок	Параметр	Возможные значения	Описание
Database	StorageType	"PostgreSql"|"SqlServer"	Тип СУБД
	ConnectionString	"Server=localhost;Database=SmevArchive.Database;Username=postgres;Pooling=True"	Строка подключения к БД
AisNalog	Enabled	"false"	Значение параметра должно быть выставлено в false
AisNalogClient	Url	http://server:port/inias/csc/gws/uc/ecpsvc/api/v1/	Адрес подключения к АИС Налог
	Credentials {UserName,Password}	Логин и пароль	Учетные данные для подключения к АИС Налог
	EnableEmulation	"false | true"	Эмуляция отправки запросов в АИС Налог
Nats	Url	"nats://<DNS>:4222"	Адрес подключения к NATS
Stan	Url ClusterID ClientID	"nats://<DNS>:4222" "pkica-cluster", "pkica-archive-service",	Адрес и параметры подключения к NATS Streaming
Smev	Url	"http://server:port/smev/v1.2/ws?wsdl"	Адрес подключения к СМЭВ
	Thumbprint	"CetificateThumbpint"	Отпечаток сертификата для подключения к СМЭВ
	FSUrl	"ftp://server"	Адрес файлового сервера СМЭВ
	LifetimeOfCertVerification	"00:00:10"	Период времени, на которое будет кэшироваться успешный результат проверки сертификата подписи ответа СМЭВ
	SuppressSmevResponseSignatureVerification	"true | false"	Отключение проверки подписи ответов СМЭВ Рекомендуемое значение: false
	StoreLocation	"CurrentUser"| "LocalMachine"	Тип хранилища
Serilog	Default	Warning|Error|Information|Verbose|Debug|Fatal	Уровень журналирования
	Microsoft		
	Microsoft.Hosting.Lifetime		
WriteTo	path	"/home/cryptopro/ecp/log/CryptoPro.SmevArchive.Service_.log"	Путь для сохранения журналов
	rollingInterval	"Day"	Создание нового журнала в указанный период времени
	retainedFileCountLimit	"7"	Сохранение последних журналов согласно указанному количеству

Блок	Параметр	Возможные значения	Описание
	fileSizeLimitBytes	"1024"	Ограничение размера файла журналов. По умолчанию: 1 Гб

7.2. Настройки веб-сервиса Проверок

Конфигурация (настройки) веб-сервиса Проверок определяются параметрами в файле appsettings.json приложения CryptoPro.SmevArchive.Web.

Таблица 4. Параметры приложения CryptoPro.SmevArchive.Web

Блок	Параметр	Возможные значения	Описание
Сетевые настройки приложения	Urls	http://localhost:5001	Адрес приложения. Если параметр не задан, по умолчанию приложение будет запущено с адресом http://localhost:5001
Nats	Url	"nats://<DNS>:4222"	Адрес подключения к NATS
ArchiveWebOptions	UseCertificateForwarding	"true"	Значение должно быть указано как true
	UseEcpNatsProxyHandlers	"false"	Для Сервиса Проверок значение должно быть выставлено в false
Database	StorageType	"PostgreSql"|"SqlServer"	Тип СУБД
	ConnectionString	"Server=localhost;Database=SmevArchive.Database;Username=postgres;Pooling=True"	Строка подключения к БД
Serilog	Default	"Warning|Error|Information|Debug"	Уровень журналирования
	Microsoft		
	Microsoft.Hosting.Lifetime		
WriteTo	path	"/home/cryptopro/ecp/log/CryptoPro.SmevArchive.Web_.log"	Путь для сохранения журналов
	rollingInterval	"Day"	Создание нового журнала в указанный период времени
	retainedFileCountLimit	"7"	Сохранение последних журналов согласно указанному количеству
	fileSizeLimitBytes	"1024"	Ограничение размера журналов. По умолчанию: 1 Гб

7.3. Настройки сервиса NATS Streaming

Конфигурация (настройки) сервиса NATS Streaming определяются параметрами в файле nats.conf приложения nats-streaming-server

Таблица 5. Параметры приложения NATS Streaming

Блок	Параметр	Возможные значения	Описание
# NATS	listen	"<DNS>:4222"	Адрес подключения к NATS
	http_port	"8222"	Адрес сервера мониторинга NATS. Без указания параметра сервер мониторинга будет выключен. Примеры адресов: • NATS http://server:port/varz • NATS Streaming (STAN) http://server:port/streaming
# NATS Streaming	cluster_id	"pkica-cluster"	Название кластера NATS Streaming
	store	"file"	Тип хранилища
	dir	"/home/cryptopro/ecp/nats-streaming/pkica-cluster-store"	Корневая директория хранилища
store limits	max_channels	50	Максимальное количество каналов к NATS. По умолчанию: 100, Неограниченное кол-во : 0
	max_bytes	5Gb	Максимальный размер сообщений для одного канала. По умолчанию 1Гб. Неограниченный размер: 0
	max_age	"360h"	Максимальный срок хранения сообщений. По умолчанию: неограниченно
	max_msgs	0	Максимальное количество сообщений в канале. По умолчанию 1 млн. Неограниченное: 0
tls			Настройка TLS между клиентом и серверов NATS (STAN) Если параметр не указан, TLS не требуется

7.4. Перечень команд утилиты pkica

Таблица 6. Перечень команд pkica

Команда	Дополнительный Параметр	Возможные значение	Описание
pkica db smev upgrade	--command-timeout «тайм-аут времени обновления БД»	pkica db smev upgrade --command-timeout 01:00	Обновление БД Сервиса Проверок
pkica smev operator add		см. 4.2	Добавление Оператора