



КриптоПро РКІ-Кластер
Шлюз прикладного уровня

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

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ	2
СОДЕРЖАНИЕ.....	3
1. Аннотация	4
2. Системные требования.....	5
2.1.Требования к аппаратному обеспечению	5
2.2.Требования к программному обеспечению.....	5
3. Развертывание Шлюза прикладного уровня	6
3.1.Установка ОС.....	6
3.2.Установка КриптоПро CSP.....	6
3.3.Развертывание веб-сервера.....	6
3.4.Установка СУБД	9
3.5.Установка ПО Шлюза прикладного уровня.....	9
4. Настройка Шлюза прикладного уровня	11
4.1.Регистрация сервисов Шлюза прикладного уровня	11
4.2.Добавление Операторов Шлюза прикладного уровня.....	11
4.3.Настройка взаимодействия с Сервисом обеспечения работы Операторов	12
4.1.Настройка взаимодействия с Сервисом Проверки Подписи	13
5. Обновление Шлюза прикладного уровня.....	13
6. Управление сервисными сертификатами	14
6.1.Пример назначения сертификата NATS Streaming	14
6.2.Пример назначения сервисных сертификатов Шлюза прикладного уровня	14
7. Дополнительные настройки компонент Шлюза прикладного уровня.....	16
7.1.Настройки сервиса Шлюза прикладного уровня	16
7.2.Настройки веб-сервиса Шлюза прикладного уровня	17
7.3.Настройки сервиса NATS Streaming	18
7.4.Перечень команд утилиты rkica	19

1. Аннотация

Настоящий документ содержит Руководство администратора Шлюза прикладного уровня ПК «КриптоПро РКІ-Кластер» (Далее – Шлюз прикладного Уровня).

Документ включает в себя описание процессов разворачивания и настройки основных технических и программных решений Шлюза прикладного уровня и предназначен для системных администраторов и Администраторов РКІ-Кластера как руководство по установке и конфигурированию РКІ-Кластера.

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ООО «КРИПТО-ПРО» Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены компанией ООО «КРИПТО-ПРО» без предварительного уведомления. Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе компания ООО «КРИПТО-ПРО» не предоставляет никаких ни явных, ни подразумеваемых гарантий. Владельцем товарных знаков КриптоПро, КРИПТО-ПРО, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ООО «КРИПТО-ПРО». Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев. Сведения, приведённые в данном документе, актуальны на дату его публикации. При перепечатке и использовании данных материалов либо любой их части ссылки на ООО «КРИПТО-ПРО» обязательны.

© 2000-2022, ООО «КРИПТО-ПРО» Все права защищены.

2. Системные требования

2.1. Требования к аппаратному обеспечению

Аппаратные требования к техническим средствам, на которых размещаются программные компоненты Шлюза прикладного уровня, зависят от количества зарегистрированных Пользователей и 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 Шлюза прикладного уровня

В данном разделе описывается развертывание Шлюза прикладного уровня. Для выполнения развертывания Шлюза прикладного уровня необходимо выполнить следующие шаги:

1. Установка ОС.
2. Установка КриптоПро CSP.
3. Установка веб-сервера.
4. Установка СУБД.
5. Установка ПО «РКИ-Кластер. Шлюз прикладного уровня» и дополнительного ПО.

3.1. Установка ОС

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



Для отображения печатных форм в Шлюзе прикладного уровня необходимо установить пакет **libgdiplus**.

3.2. Установка КриптоПро CSP

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

3.3. Развертывание веб-сервера

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

3.3.1. Пример развертывания и настройки веб-сервера nginx

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



ППО nginx не входит в комплект поставки СКЗИ. Исходные тексты nginx 1.18.0 должны быть загружены 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/cprosp/lib/amd64 -ldrdrsup -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_spki_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_spki_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 Шлюза прикладного уровня 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 Шлюза прикладного уровня в виде pfx-файла.

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

3.3.3. Конфигурация nginx для Шлюза прикладного уровня

Для обеспечения работоспособности Шлюза прикладного уровня 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 PKI-Кластера  
    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/ca {
```



```
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. Пример установки:

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

3.5. Установка ПО Шлюза прикладного уровня

3.5.1. Подготовка дистрибутива Шлюза прикладного уровня

Дистрибутив Шлюз прикладного уровня необходимо скопировать на сервер в директорию /opt/ecp/version_ecp/ (**допустимо указание другого пути**) и дать права на исполнение следующим файлам:

```
chmod u+x "/opt/ecp/version_ecp/CryptoPro.Ecp.Service/CryptoPro.Ecp.Service"
chmod u+x "/opt/ecp/version_ecp/CryptoPro.Ecp.Web/CryptoPro.Ecp.Web"
chmod u+x "/opt/ecp/version_ecp/pkica/pkica"
chmod u+x "/opt/ecp/version_ecp/pkica-test/pkica-test"
chmod u+x "/opt/ecp/version_ecp/CryptoPro.DssProxy.Service/CryptoPro.DssProxy.Service"
chmod u+x "/opt/ecp/version_ecp/CryptoPro.SvsProxy.Service/CryptoPro.SvsProxy.Service"
chmod u+x "/opt/ecp/version_ecp/CryptoPro.NatsRouter.Service/CryptoPro.NatsRouter.Service"
```

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.Ecp.Service.

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

3.5.2. Развертывание базы данных Шлюза прикладного уровня

Для разворачивания СУБД Шлюза прикладного уровня необходимо выполнить следующие команды:

```
cd "/opt/ecp/version_ecp/pkica"
```

КриптоПро РКИ-Кластер

Шлюз прикладного уровня.

Руководство администратора

```
./pkica ecp db new
```

3.5.3. Подготовка сервисных сертификатов

Для обеспечения функционирования Шлюза прикладного уровня необходимо подготовить следующие сервисные сертификаты:

1. Сертификат веб-сервера (см. 3.3.2).
2. Сертификат NATS Streaming (см. 6.1).
3. Сертификат сервиса Шлюза прикладного уровня (см. 6.2).
4. Сертификат веб-сервиса Шлюза прикладного уровня (см. 6.2).
5. Сертификат(-ы) Администратора РКІ-Кластера.
6. Сертификат для подключения к СДЭП (см. 0)

3.5.4. Запуск сервиса NATS Streaming

Для запуска сервиса NATS Streaming необходимо выполнить следующие действия:

- 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 Шлюз прикладного уровня

Для запуска сервиса Шлюз прикладного уровня в файле **appsettings.json** приложения `CryptoPro.Ecp.Service` необходимо:

- указать параметры подключения к БД `Ra.Database`:

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

- выполнить следующую команду:

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

3.5.6. Запуск веб-сервиса Шлюза прикладного уровня

Для запуска веб-сервиса Шлюз прикладного уровня в файле **appsettings.json** приложения `CryptoPro.Ecp.Web` необходимо:

- указать параметры подключения к БД `Ra.Database`:

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

- выполнить следующую команду:

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

4. Настройка Шлюза прикладного уровня

4.1. Регистрация сервисов Шлюза прикладного уровня

В разделе ниже описан процесс создания юнитов в systemd для сервисов Шлюза прикладного уровня для их автоматического управления данным сервисом. 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> приведен ниже.

```
[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 с помощью следующих команд:

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

4.2. Добавление Операторов Шлюза прикладного уровня

Для добавления оператора Шлюза прикладного уровня с правами администратора (Администратор) необходимо выполнить следующую команду:

```
./pkica ecp operator add --last-name "Иванов" --first-name "Иван" --cert-file /administrator.cer --group-name Administrators --is-admin -ipcode "код точки выдачи"
```

Для добавления оператора Шлюза прикладного уровня необходимо выполнить следующую команду:

```
./pkica ecp operator add --last-name "Петров" --first-name "Петр" --cert-file /operator.cer --group-name Operators -ipcode "код точки выдачи"
```

4.3. Настройка взаимодействия с Сервисом обеспечения работы Операторов

Для обеспечения взаимодействия с Сервисом обеспечения работы Операторов в файле **appsettings.json** сервиса CryptoPro.NatsRouter.Service необходимо добавить подключение к серверу (-ам) с компонентами Сервисов обеспечения работы Операторов. Ниже приведен пример конфигурации.

```
{
  "Routing": {
    "NatsConnections": [
      {
        "Alias": "InsideNats", //псевдоним NATS шлюза
        "Url": "nats://hostname:4222", //адрес сервера шлюза
        // настройки TLS
        "Secure": false, //включить или выключить TLS
        "Thumbprint": "371c86e32d6ef4f7d3c70a86862601d36f7e9a721", //отпечаток
клиентского сертификата
        "StoreLocation": "CurrentUser" // "LocalMachine"
      },
      {
        "Alias": "DMZNats", //псевдоним NATS Streaming Сервиса Обеспечения Операторов
        "Url": "nats://rdmzhostname:4222", //адрес сервера Сервиса Обеспечения Операторов
        // // настройки TLS
        "Secure": false, // включить TLS
        "Thumbprint": "371c86e32d6ef4f7d3c70a86862601d36f7e9a721", //
отпечаток клиентского сертификата
        "StoreLocation": "CurrentUser" // "LocalMachine"
      },
    ],
    "StanConnections": [
      {
        "Alias": "InsideStan", //псевдоним NATS Streaming (STAN) шлюза
        "Url": "nats://hostname:4222", //адрес сервера шлюза
        "ClusterID": "pkica-cluster",
        "ClientID": "pkica-router-service",
        // настройки TLS
        // "Secure": true, // включить TLS
        // "Thumbprint": "371c86e32d6ef4f7d3c70a86862601d36f7e9a721", //
отпечаток клиентского сертификата
        // "StoreLocation": "CurrentUser" // "LocalMachine"
      },
    ],
    "Routes": [
      {
        "From": "DMZNats",
        "To": "InsideNats",
        "Subjects": [
          { "Subject": "pkica.*" }
        ]
      },
    ],
  ]
}
```

4.1. Настройка взаимодействия с Сервисом Проверки Подписи

Для обеспечения взаимодействия с Сервисом Проверки Подписи в файле **appsettings.json** сервиса `CryptoPro.SvsProxy.Service` необходимо указать параметры подключения к Сервису Проверки Подписи. Ниже приведен пример конфигурации.

```
{
  "Stan": {
    "Url": "nats://ecp.cryptopro.ru:4222", // адрес подключения к Шлюзу прикладного
уровня
    "ClusterID": "pkica-cluster", // название кластера
    "ClientID": "pkica-svsproxy-service", // идентификатор клиента
    // настройки TLS
    "Secure": false, // включить TLS // включить или выключить TLS
    "Thumbprint": "371c86e32d6ef4f7d3c70a86862601d36f7e9a721", // отпечаток
клиентского сертификата // отпечаток клиентского сертификата
    "StoreLocation": "CurrentUser" // "LocalMachine" // CurrentUser | LocalMachine -
хранилище, в котором установлен клиентский сертификат
  },
  "Svs": {
    "Url": http://reporting/SVS/rest //Ссылка на API сервера SVS
  },
}
```

5. Обновление Шлюза прикладного уровня

Для обновления компонента Шлюз прикладного уровня необходимо скопировать новый дистрибутив и выполнить поочередно следующие пункты:

1. Подготовить дистрибутив Шлюза прикладного уровня (см. 3.5.1).
2. Остановить службы приложений предыдущей версии Шлюза прикладного уровня.



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

1. Создать резервную копию БД Шлюза прикладного уровня
2. Обновить версию БД используя новую версию утилиты командной строки `pkica`:

```
cd "/opt/ecp/new_version_ecp/pkica"
./pkica ecp db upgrade
```

3. Запустить службы приложений новой версии Шлюза прикладного уровня (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 **umu** от имени пользователя, под которым будут запущены сервисы.

6.2. Пример назначения сервисных сертификатов Шлюза прикладного уровня

В Шлюзе прикладного уровня сервисы NATS используют CryptoPro.Esp.Service и CryptoPro.Esp.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 уникальное 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". Можно воспользоваться утилитой certmgr:

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



Сертификаты необходимо установить в хранилище **my** 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.Esp.Web:

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

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

7. Дополнительные настройки компонент Шлюза прикладного уровня

7.1. Настройки сервиса Шлюза прикладного уровня

Конфигурация (настройки) сервиса Шлюза прикладного уровня определяются параметрами в файле appsettings.json приложения CryptoPro.Ecp.Service.

Таблица 3. Параметры приложения CryptoPro.Ecp.Service

Блок	Параметр	Возможные значения	Описание
Database	StorageType	"PostgreSql" "SqlServer"	Тип СУБД
	ConnectionString	"Server=localhost;Database=Ra.Database;Username=postgres;Pooling=True"	Строка подключения к БД
Nats	Url	"nats://<DNS>:4222"	Адрес подключения к NATS
Stan	Url ClusterID ClientID	"nats://<DNS>:4222" "pkica-cluster", "pkica-ecp-service",	Адрес и параметры подключения к NATS Streaming
EcpOptions	OwnerCheckLifetime	"07.00:00:00"	Срок действия заявки на сертификат. По умолчанию: 7 дней
	CheckOwnerMode	"AisNalogOrSmev" "AisNalogAndSmev"	Режим проверок. По умолчанию: AisNalogOrSmev, в котором общий статус проверки будет успешным, если проверка в АИС налог завершилась успешно или все проверки в СМЭВ.
	Enable01Sep2021QualSubjectName	true false	Поддержка новых требований к форме квалифицированного сертификата от 01.09.2021
	"SignCertRequest"	true false	Подпись запроса при создании и одобрении запроса на сертификат в пользовательском интерфейсе оператора
	"RevokeCertIfNotConfirmedAfter"	"05.00:00:00"	Время, через которое будет отозван сертификат, если он не будет подтвержден, в примере указано 5 дней
Serilog	Default	Warning Error Information Verbose Debug Fatal	Уровень журналирования Шлюза прикладного уровня
	Microsoft		
	Microsoft.Hosting.Lifetime		
WriteTo	path	"/home/cryptopro/ecp/logging/CryptoPro.Ecp.Service_.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 файла журналов. По умолчанию: 1 Гб

7.2.Настройки веб-сервиса Шлюза прикладного уровня

Конфигурация (настройки) веб-сервиса Шлюза прикладного определяются параметрами в файле appsettings.json приложения CryptoPro.Esp.Web.

Таблица 4. Параметры приложения CryptoPro.Esp.Web

Блок	Параметр	Возможные значения	Описание
Nats	Url	"nats://<DNS>:4222"	Адрес подключения к NATS
EcpWebOptions	SmevArchiveUri	"https://<DNS>"	Адрес для получения содержимого ответов из СМЭВ
	UseCertificateForwarding	"true"	Значение д.б. указано как true
	IsNewCertRequestOnSeparatedPage	"false true"	Отображение запросов на сертификат на отдельной странице
	UseEcpNatsProxyHandlers	"false"	Для Шлюза прикладного уровня значение должно быть выставлено в false
	EnabledCarrierUniqueFilter	["pkcs11_", "rutoken_", "jacarta_", "esmart_", "mskey_", "smartpark_", "magistra_", "ic_fk", "ic_vpn"]	Перечень разрешенных носителей в веб-интерфейсе Оператора
	UseSystemOperatorMessage	"false true"	Отображение сообщения от администратора в интерфейсе оператора
	SystemOperatorMessage	"Отсутствует подключение к СМЭВ. Необходимо обратиться к оператору "	Текст сообщения от администратора
	RevokeValidCertificateAfter	"01.00:00:00"	По умолчанию (без параметра) формируется отложенный отзыв, и он равен 5 дням. Чтобы указать параметр периода времени, через который будет отозван сертификат по-другому, нужно добавить параметр
	SignCertRequest	true false	Подпись запроса при создании и одобрении запроса на сертификат в пользовательском интерфейсе оператора
	UseDocAttachmentUI	true false	Включение/отключение пользовательского интерфейса прикрепления документов
	UseIdScanningUI	true false	Включение/отключение пользовательского интерфейса сканирования УЛ заявителя
	UseDssCertRequestCreationUI	true false	Включение/отключение пользовательского интерфейса создания ключа в СДЭП
	DataProtectionKeysFolder	"/etc/sharefolder"	Путь до общей папки для хранения ключа, используемого при создании токенов проверки подлинности веб-сайта
	DocAttachmentMaxSize	5	максимальный размер загружаемого файла, значение указывается в мегабайтах
EnabledDocAttachmentExtensions	[".pdf", ".jpg", ".jpeg", ".png", ".tiff", ".docx", ".doc", ".xlsx", ".xls", ".csv"]	разрешённые расширения загружаемых документов	
UserTemplateOid	"<OID шаблона сертификата пользователя>",	OID шаблона сертификата пользователя	
OperatorTemplateOid	"<OID шаблона сертификата оператора>"	OID шаблона сертификата оператора (шаблон, по которому будет создаваться запрос оператора)	
Database	StorageType	"PostgreSql" "SqlServer"	Тип СУБД
	ConnectionString	"Server=localhost;Database=Ra.Database;Username=postgres;Pooling=True"	Строка подключения к БД

Блок	Параметр	Возможные значения	Описание
Stan	Url	"nats://<DNS>:4222"	Адрес и параметры подключения к NATS Streaming
	ClusterID ClientID	"pkica-cluster", "pkica-ecp-web",	
EcpOptions	OwnerCheckLifetime	"07.00:00:00"	Срок действия заявки на сертификат. По умолчанию: 7 дней
	CheckOwnerMode	"AisNalogOrSmev" "AisNalogAndSmev"	Режим проверок. По умолчанию: AisNalogOrSmev, в котором общий статус проверки будет успешным, если проверка в АИС налог завершилась успешно или все проверки в СМЭВ.
	Enable01Sep2021QualS ubjectName	"true false"	Поддержка новых требований к форме квалифицированного сертификата от 01.09.2021
Serilog	Default	"Warning Error Informat ion Debug"	Уровень журналирования
	Microsoft		
	Microsoft.Hosting.Li fetime		
WriteTo	path	"/home/cryptopro/ecp/lo g/CryptoPro.Ecp.Web_.lo g"	Путь для сохранения журналов
	rollingInterval	"Day"	Создание нового журнала в указанный период времени
	retainedFileCountLim it	"7"	Сохранение последних журналов согласно указанному количеству
	fileSizeLimitBytes	"1024"	Ограничение размера файла 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: <ul style="list-style-type: none"> 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/na ts-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 ecp db upgrade	--command-timeout «тайм-аут времени обновления БД»	./pkica ecp db upgrade - -command-timeout 01:00	Обновление БД Шлюза Прикладного уровня
pkica ecp cert-request change-log	--out-file "путь для сохранения файла логов"	./pkica ecp cert-request change-log --out-file /var/log/ecp/change-log.csv	Журналирование: формирование csv файла журнала изменений новых заявок
pkica ecp operator add		См. 4.2	Добавление Оператора
pkica ecp events publish	-r "дата публикации информации об отозванных сертификата"; -n "дата публикации информации о выпущенных сертификатах"; -c "дата публикации информации о заявках на сертификат";	./pkica ecp events publish -r "01.07.2021" -n "01.07.2021" -c "01.07.2021"	Публикация данных в центр статистики
pkica ecp settings update-id-forensics	--file "путь к файлу с настройками обязательности признаков достоверности УЛ";	./pkica ecp settings update-id-forensics --file id-forensic-evidences.json	Настройка обязательности признаков достоверности УЛ
pkica ecp settings get -n IssuePointsOptions --format json	-f "путь для сохранения файла"	pkica ecp settings get -n IssuePointsOptions -f IssuePointsOptions.json --format json	Выгрузить в файл словарь точек выдачи
pkica ecp settings set -n IssuePointsOptions	-f "путь для загрузки файла"	pkica ecp settings set -n IssuePointsOptions -f IssuePointsOptions.json	Загрузить словарь точек выдачи из файла