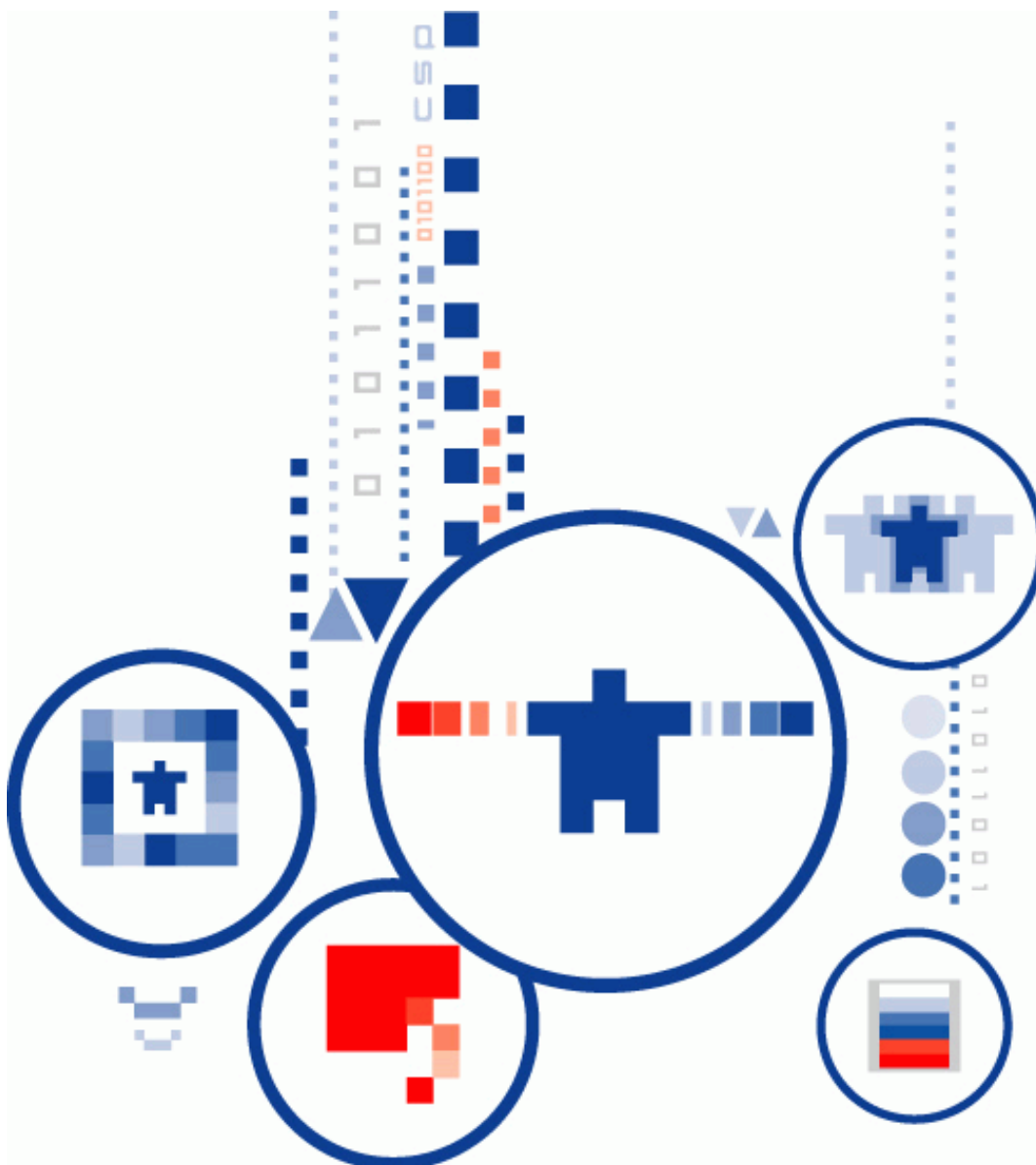




КриптоПро РКІ-Шлюз **Сервис статистики**

Инструкция по установке

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 Сервиса статистики	6
3.1. Установка и подготовка ОС	6
3.2. Настройка Центра Сертификации УЦ	Ошибка! Закладка не определена.
3.3. Изготовление сертификатов операторов ЦР	7
3.4. Разворачивание Сервиса статистики	7
3.5. Настройка карты России для страницы с точками выдачи	16

1. Аннотация

Настоящий документ содержит Руководство администратора дополнительной компоненты «Сервис статистики» (далее — Сервис статистики) из состава Программного комплекса «КриптоПро РКИ-Шлюз» (далее — КриптоПро РКИ-Шлюз) версии 1.0.

Документ включает в себя описание процессов разворачивания и настройки основных программных решений Сервиса статистики и предназначен для системных администраторов и Администраторов КриптоПро РКИ-Шлюз как руководство по установке и конфигурированию КриптоПро РКИ-Шлюз.

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. Владелец 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.

© 2000-2021, 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 Сервиса статистики, 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

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	Windows Server 2012 R2/2016/2019 (x64)
СУБД	Microsoft SQL Server 2012/2014/2016/2017
Веб-сервер	Internet Information Services, 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 статистики

В данном разделе описывается порядок развертывания Сервиса статистики. Для выполнения развертывания Сервиса статистики необходимо выполнить следующие шаги:

- Установка и подготовка ОС:
 - Установка веб-сервера IIS;
 - Установка .NET Core;
 - Установка СУБД;
 - Установка КриптоПро CSP.
- Регистрация в PKI-Шлюз точек выдачи;
- Создание и регистрация сертификатов операторов;
- Разворачивание Сервиса статистики:
 - Разворачивание БД Сервиса статистики;
 - Регистрация пользователей Сервиса статистики;
 - Настройка обмена данными с КриптоПро PKI-Шлюз;
 - Настройка КриптоПро PKI-Шлюз;
 - Настройка приложений в IIS.
- Настройка карты России для страницы с точками выдачи.

3.1. Установка и подготовка ОС

Ниже приведён примерный набор действий для подготовки компьютера с 64-битной операционной системой семейства Windows Server.

Все пути отсчитываются от корня установочного (дистрибутивного) диска КриптоПро PKI-Шлюз Сервис статистики.

3.1.1 Установка веб-сервера IIS

Установка веб-сервера IIS осуществляется посредством Диспетчера сервера путем добавления роли «Веб-сервер (IIS)» с набором служб веб-сервера по умолчанию.

В случае отсутствия доступа к DNS-серверу дополнительно потребуется прописать IP-адрес сервера Сервиса статистики и сервера КриптоПро PKI-шлюз в файл «hosts».

3.1.2 Установка .NET Core 3.1

Установка пакета размещения .NET Core 3.1 осуществляется с установочного диска.

```
C:\> E:\dotnet-hosting-3.1.9-win.exe
```

3.1.3 Установка СУБД

Дистрибутив СУБД Microsoft SQL Server необходимо получить самостоятельно. Установка нового экземпляра MSSQL и SQL Server Management Studio осуществляется согласно эксплуатационной документации с компонентами и настройками по умолчанию.

По окончании установки СУБД необходимо запустить «Диспетчер конфигурации SQL Server», перейти в раздел «Сетевая конфигурация SQL Server» и далее в «Протоколы для MSSQLSERVER». Для протокола «TCP/IP» из контекстного меню выбрать пункт «Включить», а затем пункт «Свойства». В окне «Свойства TCP/IP» перейти в закладку «IP-адреса» и в разделе «IPALL» для параметра «TCP Dynamic Ports» задать пустое значение, а для параметра «TCP Port» указать порт, отличающийся от порта 1433, назначаемого по умолчанию, например, 50500. После этого перейти в раздел «Службы SQL Server» и выполнить перезапуск службы «SQL Server (MSSQLSERVER)».

Загрузить и выполнить установку Microsoft .Net Framework 4.8.

3.1.4 Установка КриптоПро CSP

Дистрибутив необходимо получить самостоятельно. При установке КриптоПро CSP необходимо включить опцию «Криптопровайдер уровня ядра ОС».

При использовании дистрибутива CSP KC2 необходимо помнить, что требуется установка аппаратного датчика случайных чисел и ряда других мер, описанных в документации к CSP.

3.2. Регистрация в РКИ-Шлюз точек выдачи

В целях обеспечения возможности сбора сведений о созданных квалифицированных сертификатах, запросах на сертификаты, сформированных посредством КриптоПро РКИ-Шлюз, а также сведений об аннулированных сертификатах в КриптоПро РКИ-Шлюз необходимо выполнить регистрацию кодов точек выдачи операторов ФНС России и доверенных лиц ФНС России.

Код точки выдачи может состоять из нескольких чисел, разделенных точкой (формат OID'a), например, «1.52.7711.1», и текстового описания, например, «ИФНС №11 г.Москвы, АРМ №1». В записи «1.52.7711.1» первое значение до точки содержит код подчинения точки выдачи (ФНС России), второе значение – обозначение региона для точек выдачи ФНС России либо код, предназначенный для определения доверенных лиц ФНС России, третье значение – код конкретной налоговой инспекции или доверенного лица ФНС России, а четвертое – порядковый номер рабочего места точки выдачи.

Регистрация кодов точек выдачи операторов ФНС России и доверенных лиц ФНС России осуществляется в соответствии с документом КриптоПро РКИ-Шлюз Руководство администратора.

3.3. Создание и регистрация сертификатов операторов

Создание сертификатов осуществляется штатно с применением Консоли управления ЦР из состава ПАК «Удостоверяющий центр «КриптоПро УЦ».

Регистрация операторов и назначение для них сертификатов осуществляется в соответствии с документом КриптоПро РКИ-Шлюз Руководство администратора.

3.4. Разворачивание Сервиса статистики

Для разворачивания Сервиса статистики потребуется создание БД Сервиса статистики, установка и настройки модулей Сервиса статистики, обеспечивающих получение сведений из КриптоПро PKI-Шлюз, а также предоставляющих возможность доступа к данным Сервиса статистики через сеть.

Ниже представлены разделы, описывающие особенности создания БД Сервиса статистики, а также установку и настройку указанных модулей.

3.4.1 Разворачивание БД Сервиса статистики

Необходимо проверить, что на сервере установлен Microsoft .Net Framework 4.8. Далее в среде SQL Server Management Studio выполнить скрипт:

```
EXEC sp_configure 'show advanced options', 1
RECONFIGURE;
EXEC sp_configure 'clr strict security', 0
RECONFIGURE;
EXEC sp_configure 'clr enabled', 1
RECONFIGURE;
```

Для разворачивания базы данных Сервиса статистики необходимо перейти в каталог pkica установочного дистрибутива, задать в конфигурационном файле appsettings.json для раздела «StatDatabase» параметры подключения к БД и выполнить следующую команду от имени у четной записи, являющейся членом группы sysadmin экземпляра MS SQL Server:

```
pkica stat db new
```

После создания БД Сервиса статистики необходимо заполнить справочник точек выдачи, а также справочники федеральных округов, субъектов Российской Федерации и доверенных лиц ФНС России путем выполнения в среде SQL Server Management Studio скриптов из приведенных ниже файлов строго в указанном порядке:

```
insert_federal_districts_and_subjects.sql
insert_issuer_points.sql
add_partners.sql
```

При необходимости имеется возможность добавить в справочник тестовые точки выдачи, выполнив следующие команды (строго после выполнения предыдущих скриптов):

```
INSERT INTO IssuePoint (IssuePointCode, Name, FederalSubjectCode, Latitude,
Longitude)
VALUES('1.6.5505', 'Инспекция ФНС России № 10', '10', 61.799685, 34.357102)
INSERT INTO IssuePoint (IssuePointCode, Name, FederalSubjectCode, Latitude,
Longitude)
VALUES('1.1.7710', 'Инспекция ФНС России № 11', '10', 62.198897, 34.262859)
INSERT INTO IssuePoint (IssuePointCode, Name, FederalSubjectCode, Latitude,
Longitude)
VALUES('1.2.7807', 'Инспекция ФНС России № 12', '10', 61.702997, 30.688259)
```


Для миграции существующей базы данных Сервиса статистики на новую версию необходимо создать ее резервную копию и выполнить следующую команду:

```
pkica stat db upgrade
```

3.4.2 Регистрация пользователей Сервиса статистики

Для регистрации пользователей Сервиса статистики необходимо перейти в каталог `pkica` и выполнить команду «`pkica stat user add`» от имени у четной записи, являющейся членом группы `sysadmin` экземпляра MS SQL Server. Пример использования команды:

```
pkica stat user add --login TestUser -p password -l Иванов -f Иван -m Иванович
```

где «`TestUser`» - логин пользователя, а «`password`» - пароль.



Пароль должен иметь длину не менее 6 символов и удовлетворять требованиям к сложности: содержать заглавные и строчные буквы английского алфавита, а также хотя бы один спецсимвол.

Для удаление ранее зарегистрированного пользователя следует выполнить команду `pkica stat user delete --login <логин пользователя>`.

3.4.3 Настройка обмена данными с КриптоПро PKI-Шлюз

Получение сведений Сервисом статистики из КриптоПро PKI-Шлюз осуществляется посредством сервиса `nuts-streaming` - системы обмена сообщениями, которая обеспечивает обмен данными между КриптоПро PKI-Шлюз и Модулем записи сертификатов (`CryptoPro.Stat.Service`). Сервис `nuts-streaming` разворачивается как на КриптоПро PKI-Шлюз, так и на сервере Сервиса статистики.

Сервис `nuts-streaming` устанавливается простым копированием и способен работать как отдельное приложение, так и как служба ОС Windows.

Для развертывания `nuts-streaming` на сервере Сервиса статистики необходимо перенести содержимое каталога «`nuts-streaming`» с установочного диска в корневой раздел сервера Сервиса статистики, например, в «`C:\nuts-streaming`». Далее перейти в каталог «`C:\nuts-streaming`» и в файле «`nuts.conf`» оставить только следующие блоки:

```
# NATS
listen:          stat-rDMZ:1433 # имя сервера Статистики и порт обмена информацией
                                     #с КриптоПро PKI-шлюз (1433)
max_payload:     20Mb

# NATS Streaming
cluster_id:      "pkica-cluster-rDMZ" # уникальное имя кластера Сервиса статистики
store:           "file"
dir:             "C:/nats-streaming/pkica-cluster-store"

store_limits: {
    max_channels: 50
    max_bytes:   5GB
    max_age:     "720h" # 30 дней
```

```
}
```

указав в строчке «listen:» имя сервера Сервиса статистики и порт «1433» (указанный порт разрешен для отправки данных из сетевого сегмента с серверами КриптоПро РКІ-Шлюз в сегменты с серверами Сервиса статистики), а также уникальное имя кластера Сервиса статистики, например, «pkica-cluster-rDMZ».

Запуск сервиса nuts-streaming в качестве приложения может быть осуществлен из консоли cmd путем выполнения следующей команды:

```
C:\nats-streaming> nuts-streaming-server.exe -sc nats.conf
```

Для регистрации и удаления службы можно воспользоваться следующими командами:

```
sc.exe create EcpFnsNatsStreaming start= auto binPath= " C:\nats-streaming\nats-streaming-server.exe -sc C:\nats-streaming\nats.conf"
sc.exe description EcpFnsNatsStreaming "Служба NATS Streaming Сервиса статистики ФНС"
sc.exe start EcpFnsNatsStreaming
```

Для регистрации и удаления службы можно воспользоваться следующими командами:

```
stat-nuts-delete.bat - удаляет регистрацию службы NATS.
```

При необходимости повторить указанные действия для дополнительных серверов Сервиса статистики, указав порт «1433» и уникальное имя кластера Сервиса статистики, например, «pkica-cluster-iDMZ».

Модуль CryptoPro.Stat.Service получает сведения от сервиса nuts-streaming, установленного на сервере Сервиса статистики, по созданным и аннулированным сертификатам, а также выполняет их запись в БД Сервиса статистики. Модуль записывает в БД только сертификаты, для которых указаны код точки выдачи и поля, по которым можно определить тип сертификата (ИНН, ОГРНИП).

Модуль устанавливается простым копированием и способен работать как отдельное приложение, так и как служба ОС Windows.

Для установки модуля необходимо с установочного дистрибутива перенести папку CryptoPro.Stat.Service на сервер Сервиса статистики и задать в конфигурационном файле appsettings.json значения для следующих параметров:

- «ConnectionString» в блоке «Database» - строка подключения к БД Сервиса статистики, установленный для SQL Server порт допускается не указывать при включенной службе «Обозреватель SQL Server»;
- «Url» в блоке «Stun» - URL подключения к сервису nuts-streaming (в данном примере: «stat-rDMZ:1433»);
- «ClusterID» в блоке «Stun» - уникальное имя кластера Сервиса статистики, заданное ранее в конфигурационном файле nats.conf сервиса nuts-streaming («pkica-cluster-rDMZ»);
- «ThreadCount» в блоке «StatOptions» - количество потоков-обработчиков (если задано значение меньше 1, то количество потоков будет равно количеству логических процессоров);

- «IdempotencyPeriod» в блоке «StatOptions» - период, в течение которого обеспечивается идемпотентная обработка событий о создании и аннулировании сертификатов. Вновь пришедшие события старше этого возраста могут быть обработаны повторно (параметр указывается в формате промежутка времени dd.hh:mm:ss, где dd - дни, hh - часы, mm - минуты, ss - секунды);
- «CommandTimeout» в блоке «StatOptions» - таймаут выполнения операций с БД Сервиса статистики (значение необходимо указывать в секундах).

Также в блоке «Serilog» конфигурационного файла можно изменить уровень журналирования (Error, Warning, Information, Verbose). По умолчанию лог (журнал) пишется в файл C:\log\CaStat.Service_ГГГГММДД.log, где «ГГГГММДД» содержит соответственно сведения о годе, месяце и дате создания лог-файла.

Модуль может быть запущен как отдельное приложение, либо как служба ОС Windows.



Для начального запуска и отладки удобно изменить уровень журналирования на Information и запускать модуль как отдельное приложение (информация о работе модуля будет выводиться в консольном окне). Не забудьте после отладки изменить уровень журналирования на Warning.

Запуск модуля в качестве приложения может быть осуществлен из консоли cmd путем выполнения файла CryptoPro.Stat.Service.exe без параметров запуска.

Для регистрации и удаления службы можно воспользоваться следующими скриптами:

```
stat-service-create.bat - выполняет регистрацию службы StatSrv;
stat-service-delete.bat - удаляет регистрацию службы StatSrv.
```

Служба запускается под системной учетной записью. Разрешить службе взаимодействовать с БД Сервиса статистики можно с помощью следующего скрипта (выполнять на БД Сервиса статистики):

```
CREATE USER [NT AUTHORITY\СИСТЕМА] FOR LOGIN [NT AUTHORITY\СИСТЕМА]
ALTER ROLE [db_owner] ADD MEMBER [NT AUTHORITY\СИСТЕМА]
```

3.4.4 Настройка КриптоПро PKI-Шлюз

Направление сведений Сервису статистики со стороны кластера КриптоПро PKI-Шлюз осуществляется посредством сервиса nuts-streaming. Для его настройки необходимо проверить подключение к сервису nuts-streaming, развернутому на одном или на нескольких серверах Сервиса статистики, путем выполнения следующей команды на каждом узле кластера КриптоПро PKI-Шлюз:

```
telnet hostname 1433
```

где в качестве «hostname» указывается имя сервера Сервиса статистики («stat-rDMZ»).

Далее добавить в файл «appsettings.json» приложения «CryptoPro.Esp.Service» на первом узле кластера КриптоПро PKI-Шлюз следующий раздел:

```
"Routing": {
  "NatsConnections": [
    {
      "Alias": "InsideNats",
      "Url": "nats://n5001-cas021:4222", // n5001-cas021 - имя сервера
      //КриптоПро PKI-Шлюз
      // настройки TLS
      "Secure": false, // включить TLS
      "Thumbprint": "371c86e32d6ef4f7d3c70a86862601d36f7e9a721", // отпечаток
      клиентского сертификата
      "StoreLocation": "CurrentUser" // "LocalMachine"
    },
    {
      "Alias": "iDMZNats",
      "Url": "nats://stat-iDMZ:1433",
      // настройки TLS
      "Secure": false, // включить TLS
      "Thumbprint": "371c86e32d6ef4f7d3c70a86862601d36f7e9a721", // отпечаток
      клиентского сертификата
      "StoreLocation": "CurrentUser" // "LocalMachine"
    },
    {
      "Alias": "rDMZNats",
      "Url": "nats://stat-rDMZ:1433",
      // настройки TLS
      "Secure": false, // включить TLS
      "Thumbprint": "371c86e32d6ef4f7d3c70a86862601d36f7e9a721", // отпечаток
      клиентского сертификата
      "StoreLocation": "CurrentUser" // "LocalMachine"
    }
  ],
  "StanConnections": [
    {
      "Alias": "InsideStan",
      "Url": "nats://n5001-cas021:4222",
      "ClusterID": "pkica-cluster",
      "ClientID": "pkica-router-service",
      // настройки TLS
      "Secure": false, // включить TLS
      "Thumbprint": "371c86e32d6ef4f7d3c70a86862601d36f7e9a721", // отпечаток
      клиентского сертификата
      "StoreLocation": "CurrentUser" // "LocalMachine"
    },
    {
      "Alias": "iDMZStan",
      "StartAt": "2021-12-28T00:00:00+03:00", // время старта сбора статистики
      "Url": "nats://stat-iDMZ:1433",
      "ClusterID": "pkica-cluster-iDMZ",
```

```

        "ClientID": "pkica-router-service",
        // настройки TLS
        "Secure": false, // включить TLS
        "Thumbprint": "371c86e32d6ef4f7d3c70a86862601d36f7e9a721", // отпечаток
клиентского сертификата
        "StoreLocation": "CurrentUser" // "LocalMachine"
    },
    {
        "Alias": "rDMZStan",
        "StartAt": "2021-12-28T00:00:00+03:00", // время старта сбора статистики
        "Url": "nats://stat-rDMZ:1433",
        "ClusterID": "pkica-cluster-rDMZ",
        "ClientID": "pkica-router-service",
        // настройки TLS
        "Secure": false, // включить TLS
        "Thumbprint": "371c86e32d6ef4f7d3c70a86862601d36f7e9a721", // отпечаток
клиентского сертификата
        "StoreLocation": "CurrentUser" // "LocalMachine"
    }
],

"Routes": [
    {
        "From": "InsideNats",
        "To": "iDMZNats",
        "Subjects": [
            { "Subject": "pkica.ra.command.settings.changed" }
        ]
    },
    {
        "From": "InsideNats",
        "To": "rDMZNats",
        "Subjects": [
            { "Subject": "pkica.ra.command.settings.changed" }
        ]
    },
    {
        "From": "InsideStan",
        "To": "iDMZStan",
        "Subjects": [
            // в сервер статистики
            { "Subject": "pkica.ra.command.certrequest.received" },
            { "Subject": "pkica.ra.command.certificate.issued" },
            { "Subject": "pkica.ra.command.certificate.revoked" }
        ]
    },
    {
        "From": "InsideStan",
        "To": "rDMZStan",
        "Subjects": [
            // в сервер статистики
            { "Subject": "pkica.ra.command.certrequest.received" },
            { "Subject": "pkica.ra.command.certificate.issued" },
            { "Subject": "pkica.ra.command.certificate.revoked" }
        ]
    }
]

```

```

    ]
  }
]
},

```

Для второго узла кластера КриптоПро PKI-Шлюз в файл «appsettings.json» приложения «CryptoPro.Ecp.Service» вносится аналогичный раздел, при этом для параметра «ClientID» требуется указать уникальный идентификатор, например «pkica-router-service2».

После этого потребуется перезапуск приложений «CryptoPro.Ecp.Web.service» и «CryptoPro.Ecp.service» путем выполнения следующих команд:

```

sudo systemctl restart CryptoPro.Ecp.Web.service
sudo systemctl restart CryptoPro.Ecp.service

```

3.4.5 Настройка приложений в IIS

Для настройки приложений Сервиса статистики в IIS поместить папки CryptoPro.Stat.Web.Api и CryptoPro.Stat.Web.Ui с файлами для сайта Сервиса статистики из состава установочного дистрибутива в каталог веб-сервера IIS (по умолчанию каталог IIS - C:\inetpub\wwwroot) и перейти в неё.

Для указанных папок дать права на чтение и выполнение для пользователя IUSR. Для этого следует для каждой из папок кликнуть правой кнопкой мыши, из контекстного меню выбрать «Свойства», перейти во вкладку «Безопасность» и добавить пользователя «IUSR» с правами на список содержимого папки, чтение, чтение и выполнение.

Для защиты сайта Сервиса статистики и аутентификационных данных пользователей Сервиса статистики на стороне сервера применяются два сертификата:

- Сертификат веб-сервера;
- Сертификат защиты аутентификационных данных пользователей.

Указанные сертификаты необходимо подготовить и перенести на Сервис статистики заранее. Требования к сертификатам приведены в Таблице 3.

Таблица 3. Требования к сертификатам

Назначение	Алгоритм	Требования
Сертификат веб-сервера	RSA / ГОСТ Р 34.10/11-2012	расширение «Дополнительное имя субъекта» (SAN) должно содержать DNS-имя сервера, расширении «Улучшенный ключ» (EKU) должно содержать «Проверка подлинности сервера» (1.3.6.1.5.5.7.3.1)

Назначение	Алгоритм	Требования
Сертификат защиты аутентификационных данных (подписи jwt-токена)	ГОСТ Р 34.10/11-2012	расширении «Использование ключа» (KU) должно содержать Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных

Сертификаты устанавливаются в хранилище «Личное» в контексте локального компьютера.

В Диспетчере служб IIS:

- для сайта (по умолчанию Default Web Site), на котором будут созданы веб-приложения Сервиса статистики, настроить использование сертификата веб-сервера для типа привязки https;
- перейти в «Пулы приложений» и создать пул приложений «StatWebApi» без управляемого кода. Для созданного пула открыть дополнительные параметры и указать удостоверение личности «LocalService»;
- через пункт контекстного меню «Преобразовать в приложение» преобразовать папку «CryptoPro.Stat.Web.Api» в приложение IIS, указав для приложения пул «StatWebApi». В параметрах созданного приложения перейти в «Параметры SSL» и указать галку «Требовать SSL». Радиокнопку в подразделе «Сертификаты клиента» оставить в положении «Игнорировать»;
- для доступа пула приложений «StatWebApi» к БД Сервиса статистики необходимо в среде SQL Server Management Studio выполнить следующий скрипт (выполнять на БД Сервиса статистики):

```
CREATE USER [NT AUTHORITY\LOCAL SERVICE] FOR LOGIN [NT AUTHORITY\LOCAL SERVICE]
ALTER ROLE [db_owner] ADD MEMBER [NT AUTHORITY\LOCAL SERVICE]
```

- в каталоге «CryptoPro.Stat.Web.Api» открыть конфигурационный файл «appsettings.json», в блоке «Database» для параметра «ConnectionString» указать данные для подключения к БД Сервиса статистики и внести в файл следующий блок:

```
"StatWebOptions": {
  // LocalMachine | CurrentUser - тип хранилища, в котором установлен сертификат
  "StatAuthCertStoreLocation": "LocalMachine",
  // отпечаток сертификата для подписи jwt-токена
  "StatAuthCertThumbprint": "60f8787e3a0b91116c73360892bdd040baa10024"
  // false | true - определение необходимости использования https
  "RequireHttps": true,
},
```

где в поле «StatAuthCertThumbprint» указать отпечаток сертификата, созданного в соответствии с криптографическим алгоритмом ГОСТ Р 34.10/11-2012 и предназначенного для защиты аутентификационных данных пользователей Сервиса статистики (подписи jwt-токенов);

- через пункт «Управление закрытыми ключами...» оснастки «Сертификаты» предоставить доступ к ключу ЭП (предназначенному для защиты аутентификационных данных пользователей) доступ со стороны учетной записи, от которой будет запущен пул «StatWebApi» («Local Service»);
- перейти в «Пулы приложений» и создать пул приложений «StatWebUi» без управляемого кода;

- через пункт контекстного меню «Добавить приложение» добавить в IIS приложение для сайта, указав в качестве его псевдонима «CAStat», физический путь к папке «CryptoPro.Stat.Web.Ui» и пул приложений «StatWebUi». В параметрах созданного приложения перейти в «Параметры SSL» и указать галку «Требовать SSL». Радиокнопку в подразделе «Сертификаты клиента» оставить в положении «Игнорировать»;
- в файле «config.js» папки «CryptoPro.Stat.Web.Ui» заменить имя «fns-stand» на DNS-имя машины, на которой был опубликован сайт Сервиса статистики, для параметров API_HOST и API_AUTH_HOST;

После проведения указанных настроек запустить сайт Сервиса статистики по адресу <https://fns-stand/CAStat/login.html>, где вместо «fns-stand» использовать имя машины, на которой сайт был опубликован.

На странице с предложением ввода логина и пароля пользователя указать аутентификационные данные ранее зарегистрированного пользователя Сервиса статистики, нажать кнопку «Вход» и проверить отображение основных разделов сайта Сервиса статистики.

3.5. Настройка карты России для страницы с точками выдачи

Для настройки карты России для страницы сайта Сервиса статистики необходимо скопировать из установочного дистрибутива папку `russia_tiles_png` на сервер Сервиса статистики. Данная папка большая по объёму. При наличии достаточного объема свободного места на диске C, поместите её в папку `C:\intepub\wwwroot`. В качестве альтернативы допустимо размещение папки в ином каталоге, при этом для такого каталога потребуется предоставить те же права доступа, что и для папки `wwwroot`.

В Диспетчере служб IIS в контекстном меню от «Пулы приложений» выбрать пункт «Добавить пул приложений» и указать в качестве имени «RussiaTilesAppPool». Для созданного пула приложений выбрать из контекстного меню пункт «Дополнительные параметры» и для параметра «Удостоверение» выбрать встроенную учётную запись `LocalService`.

Для создания приложения перейти в папку сайта, нажать правой кнопкой мыши на `Default Web Site` и выбрать пункт «Добавить приложение». Указать имя приложения `russia_tiles_png`, выбрать пул приложений «RussiaTilesAppPool» и нажать на кнопку OK.

Открыть файл `config.js` в папке «CryptoPro.Stat.Web.Ui» и в строке с параметром `PATH_MAP_TILES` заменить значение `fns-stand` на имя машины, на которой был развёрнут сайт:

```
const PATH_MAP_TILES = 'http://fns-stand/russia_tiles_png';
```