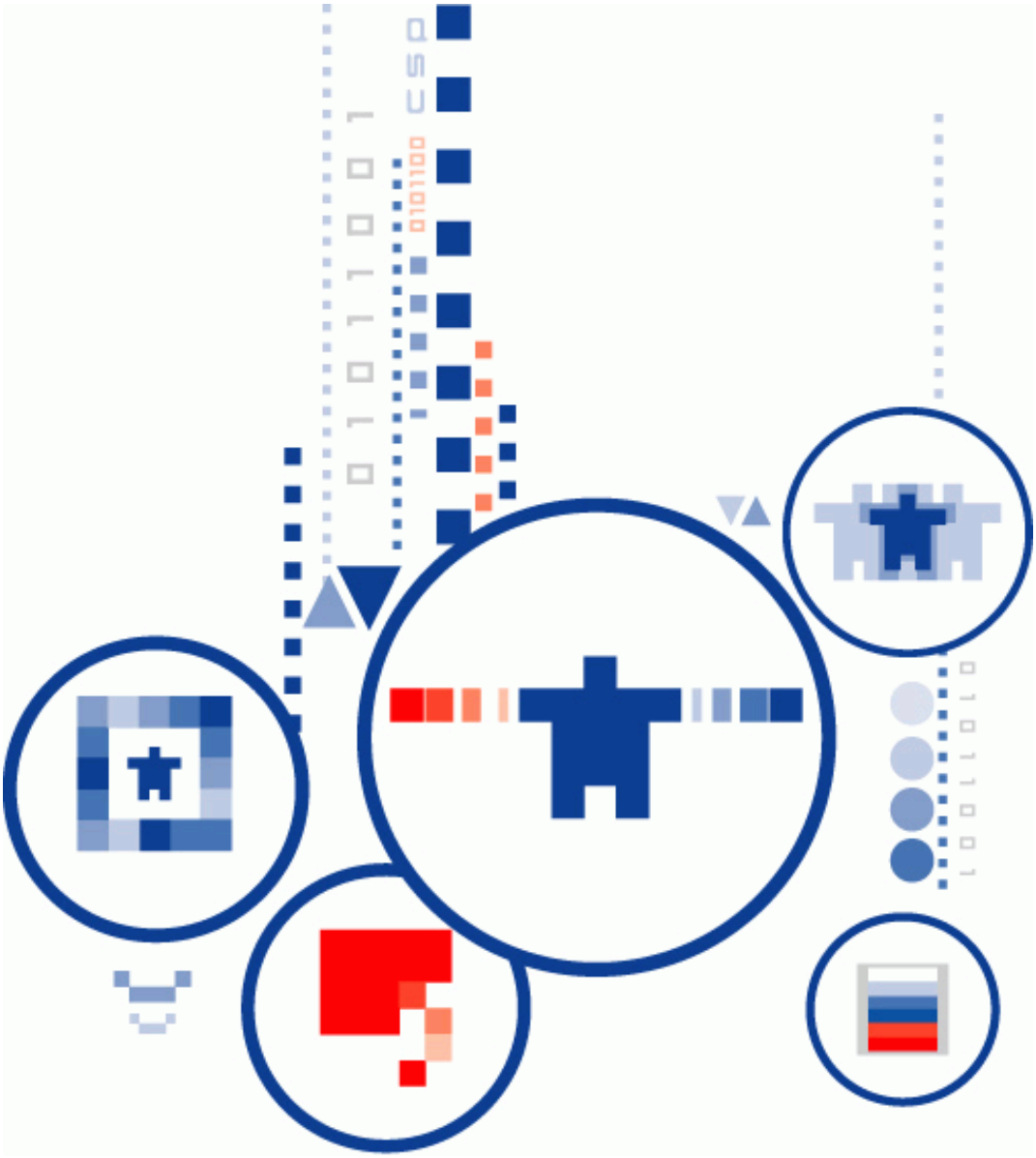

КриптоПро PKI-Кластер
Сервис взаимодействия с УЦ

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 взаимодействия с УЦ ПК «КриптоПро PKI-Кластер» (Далее – Сервис взаимодействия с УЦ).

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

2. Системные требования

2.1. Требования к аппаратному обеспечению

Аппаратные требования к техническим средствам, на которых размещаются программные компоненты Сервиса взаимодействия с УЦ, 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
Антивирусное ПО	В соответствии с эксплуатационной документацией на СКЗИ
СКЗИ	КриптоПро CSP 5.0 R2

3. Развертывание Сервиса взаимодействия с УЦ

В данном разделе описывается развертывание Сервиса взаимодействия с УЦ. Для выполнения развертывания Сервиса взаимодействия с УЦ «с нуля» необходимо выполнить следующие шаги:

1. Установка ОС.
2. Установка КриптоПро CSP.
3. Установка ПО Сервиса взаимодействия с УЦ.

3.1. Установка ОС

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

3.2. Установка КриптоПро CSP

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

3.3. Установка ПО Сервиса взаимодействия с УЦ

3.3.1. Подготовка дистрибутива Сервиса взаимодействия с УЦ

Дистрибутив Сервиса взаимодействия с УЦ необходимо скопировать на сервер в директорию /opt/ecp/version_ecp/ (**допустимо указание другого пути**) и дать право на исполнение:

```
chmod u+x
"/opt/ecp/version_ecp/CryptoPro.CaProxy.Service/CryptoPro.CaProxy.Service"
```

В директории приложения располагается конфигурационный файл **appsettings.json**. В файле **appsettings.json** необходимо указать путь (path) для сохранения логов приложений. Ниже указан пример:

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

3.3.2. Подготовка сервисных сертификатов

Для обеспечения функционирования Сервиса взаимодействия с УЦ необходимо подготовить следующие сервисные сертификаты:

1. Сертификаты Сервиса взаимодействия с УЦ (см. 6.1);
2. Сертификат для подключения к УЦ.

3.3.3. Запуск Сервиса взаимодействия с УЦ

Для запуска Сервиса взаимодействия с УЦ в файле **appsettings.json** сервиса CaProxy.Service необходимо выполнить следующую команду:

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

4. Настройка Сервиса взаимодействия с УЦ

4.1. Регистрация Сервиса взаимодействия с УЦ

В данном разделе описан процесс создания юнита в systemd Сервиса взаимодействия с УЦ для управления данным сервисом. Для этого необходимо выполнить следующие действия.

- Создать для сервиса файл в следующей директории:

```
/etc/systemd/system/CryptoPro.CaProxy.service
```

- Применить изменения:

```
sudo systemctl daemon-reload
```

- Разрешить автозагрузку:

```
sudo systemctl enable CryptoPro.CaProxy.Service
```

- Запустить сервис:

```
sudo systemctl start CryptoPro.CaProxy.Service
```

- Пример файла **CryptoPro.CaProxy.service**:

```
[Unit]
Description=CryptoPro.CaProxy.Service
[Service]
WorkingDirectory=/opt/ecp/ecp_cersion/CryptoPro.CaProxy.Service
ExecStart=/opt/ecp/ecp_version/CryptoPro.CaProxy.Service
\CryptoPro.CaProxy.Service
Restart=always
# Restart service after 10 seconds if the dotnet service crashes:
RestartSec=10
KillSignal=SIGINT
SyslogIdentifier=CryptoPro.CaProxy.Service
User=cp
[Install]
WantedBy=multi-user.target
```

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

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

4.2. Настройка подключения к УЦ

Для обеспечения взаимодействия с УЦ в файле **appsettings.json** сервиса CryptoPro.CaProxy.Service необходимо указать параметры подключения к Центру Регистрации КриптоПро УЦ 2.0. Ниже приведен пример конфигурации.

```
"Ca20Connection": {
    "Thumbprint": "f8a0a59e0d88bf5bda01a6eb4862a9149b25bbc9", # отпечаток для подключения к ЦР
    "Url": "https://localhost/RA", # адрес для подключения ЦР
    "FolderId": "ac6500cc-9034-4884-8b51-ab4a00692220", # идентификатор папки ЦР
    "DefaultTemplateName":  "User" # наименование шаблона
  },
```

Для настройки подачи запросов на сертификаты, выпускаемые операторам, в папку ЦР отличную от папки по умолчанию, необходимо в appsettings.json приложения CryptoPro.CaProxy.Service добавить в разделе Ca20Connection сопоставление идентификаторов шаблона к папкам ЦР

```
"Ca20Connection": {
"TemplateToFolderMap": [
{
"TemplateOidOrName": "<oid или имя шаблона>",
"FolderId": "<идентификатор папки>"
},
...
]
}
```

4.3. Настройка подключения к Шлюзу прикладного уровня

Для обеспечения взаимодействия с Шлюзом прикладного уровня в файле **appsettings.json** сервиса CryptoPro.CaProxy.Service в секции Stan необходимо указать параметры подключения. Ниже приведен пример конфигурации:

```
"Stan": {
    "Url": "nats://<server>:4222", // DNS-имя сервера Шлюза прикладного уровня
    "ClusterID": "pkica-cluster",
    "ClientID": "pkica-proxy-service",
    // настройки TLS
    "Secure": true, // включить TLS
    "Thumbprint": "371c86e32d6ef4f7d3c70a86862601d36f7e9a721", // отпечаток сервисного сертификата Сервиса взаимодействия с УЦ
    "StoreLocation": "CurrentUser" // "LocalMachine"
  },
```

5. Обновление Сервиса взаимодействия с УЦ

Для обновления Сервиса взаимодействия с УЦ необходимо скопировать новый дистрибутив и выполнить поочередно следующие пункты:

1. Подготовка дистрибутива Сервиса взаимодействия с УЦ (см. 3.3.1).
2. Остановить службу предыдущей версии Сервиса взаимодействия с УЦ.
3. Запустить службу новой версии Сервиса взаимодействия с УЦ (см. 3.3.3).

6. Управление сервисными сертификатами

6.1. Пример назначения сервисного сертификата Сервиса взаимодействия с УЦ

В Сервисе взаимодействия с УЦ для подключения к серверу Шлюза прикладного уровня используются сервисы NATS. 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". 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 существующий раздел и Stan:

```
"Stan": {
  "Url": "nats://<server>:4222", // DNS-имя сервера Шлюза прикладного уровня
  ...
  "Secure": true,
  "Thumbprint": "<отпечаток сервисного сертификата>"
},
```

7. Дополнительные настройки Сервиса взаимодействия с УЦ

Конфигурация (настройки) сервиса взаимодействия с УЦ определяются параметрами в файле appsettings.json приложения CryptoPro.CaProxy.Service.

Таблица 3. Параметры приложения CryptoPro.CaProxy.Service

Блок	Параметр	Возможные значения	Описание
ProxyOptions	StanBackoffThreadCount	"10"	Количество ниток обработки сообщений с УЦ
	AckTimeout	"00:05:00"	Время ожидания подтверждения обработки сообщения из очереди NATS Streaming
Ca20Connection	Thumbprint	"Отпечаток сертификата"	Отпечаток сертификата подключения к УЦ 2.0.
	StoreLocation	"CurrentUser"|"LocalMachine"	Расположение хранилища сертификата для подключения к УЦ 2.0.
	Url	"https://DNS/RA"	Адрес подключения к УЦ 2.0 (Центр Регистрации)
	FolderId	"идентификатор папки"	Идентификатор папки центра регистрации УЦ 2.0
	DefaultTemplateName	"User"	Шаблон, который будет использован, если в пришедшем запросе на сертификат шаблон не будет указан
	CheckRegRequestStatusIntervals	["00:00:00", "00:00:02", "00:00:05"]	Интервалы опроса статуса запроса на регистрацию
	WaitRegRequestProcessTimeout	"00:01:00"	Период ожидания обработки запроса на регистрацию
	CheckCertRequestStatusIntervals	["00:00:01", "00:00:02", "00:00:05"]	Интервалы опроса статуса запроса на сертификат
	WaitCertRequestProcessTimeout	"00:01:00"	Период ожидания обработки запроса на сертификат
	CheckRevRequestStatusIntervals	["00:00:01", "00:00:02", "00:00:05"]	Интервалы опроса статуса запроса на отзыв
	WaitRevRequestProcessTimeout	"00:01:00"	Период ожидания обработки запроса на отзыв
	TemplateToFolderMap	**См. Раздел 4.2**	
Stan	Url ClusterID ClientID	"nats://<DNS>:4222" "pkica-cluster", "pkica-proxy-service",	Адрес и параметры подключения к NATS Streaming (см. 0)
Serilog	Default	Warning|Error|Information|Verbose|Debug|Fatal	Уровень журналирования
	Microsoft		
	Microsoft.Hosting.Lifetime		
WriteTo	path	"/home/cryptopro/ecp/log/CaProxy.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