

Центр Управления Гетерогенными Инфраструктурами

Система централизованного анализа и
управления гетерогенными
инфраструктурами — Clearway CA

Архитектура программного обеспечения

ООО «Клируэй Текнолоджис»

Москва 2025

Содержание

1.	Введение	6
2.	Функции Clearway CA.....	7
3.	Логическая архитектура системы.....	8
3.1.	Программные компоненты системы.....	8
3.2.	Описание архитектуры Clearway CA	10
3.3.	Описание архитектуры веб-интерфейса Clearway CA.....	11
3.4.	Описание архитектуры mOSCP.....	12
3.5.	Сторонние программные компоненты	13
3.6.	Алгоритм типовой операции.....	13
4.	Физическая архитектура	15
4.1.	Типовые конфигурации	15
4.2.	Технические требования	19
4.2.1.	Рекомендуемые технические требования к серверному оборудованию	19
4.2.2.	Требования к АРМ оператора	21
4.2.3.	Требования к системному ПО	21
4.2.4.	Требование к сети	22
4.2.5.	Требования к учётным записям.....	23
4.2.6.	Группы	24
4.2.7.	Дополнительно	25
5.	Обеспечение безопасности	26
5.1.	Защита ключа ЦС.....	26
5.2.	Защита файлов системы	26
5.3.	Защита БД	26
5.4.	Защита сетевых взаимодействий	27
5.5.	Ролевая модель.....	27
5.5.1.	Ролевая модель, Control Panel.....	27
5.5.2.	Ролевая модель Clearway CA	28

Перечень терминов и сокращений

Сокращение	Расшифровка	Описание
API	Application Programming Interface	Прикладной программный интерфейс компонента ИС.
CLR	Certificate Revocation List	Список отозванных сертификатов, публикуемый Центром Сертификации
CSR	Certificate Signing Request	Запрос на подпись сертификата в формате PKCS#10, содержащий публичный ключ и атрибуты субъекта.
DeltaCRL		Инкрементальный список отозванных сертификатов, содержащий изменения с момента предыдущего CRL
HSM	Hardware Security Module	Аппаратный модуль хранения и защиты секретных ключей. При наличии интеграции HSM рассматривается как отдельный компонент/артефакт
JWT	JSON Web Token	Открытый стандарт (RFC 7519), определяющий компактный и самодостаточный способ передачи информации между сторонами в виде JSON-объекта, подписанного цифровой подписью или зашифрованного.
KRA	Key Recovery Agent	Пользователь, имеющий специальный сертификат и права для резервного копирования и восстановления криптографических ключей и цифровых сертификатов.
OCSP	Online Certificate Status Protocol	Протокол запроса статуса сертификата и получения ответа (mOCSP — OCSP-респондер в составе Clearway CA)
PKCS#10		Стандарт формата CSR
PKI (ИОК)	Public Key Infrastructure	Инфраструктура открытых ключей (ИОК) — набор средств, распределенных служб и компонентов, используемых для поддержки крипто-задач (шифрования, аутентификации, подписи) на основе закрытого и открытого ключей.
RSA	Rivest - Shamir - Adleman	Реализация криптосистемы на основе закрытого и открытого ключей.
SCEP	Simple Certificate Enrollment Protocol	протокол автоматизированного выдачи сертификатов для устройств
SSL	Secure Socket Layers	Криптографический протокол, обеспечивающий организацию безопасной сетевой связи между клиентом и сервером и упрощенной проверкой

Сокращение	Расшифровка	Описание
		подлинности сторон связи с применением сертификатов x509.
TLS / mTLS	Transport Level Security / mutual Transport Level Security —	Развитие протокола SSL, криптографический протокол на основе сертификатов x509, обеспечивающий организацию безопасной сетевой связи и взаимную аутентификацию клиента и сервера.
X.509v3		Версия международного стандарта, определяющая структуру цифровых сертификатов, содержащих информацию о субъекте (пользователе, устройстве или организации), открытый ключ субъекта и дополнительные расширения, используемые для настройки поведения сертификата и улучшения функциональности. Является основой современных методов аутентификации и защиты данных в интернет-коммуникациях, включая TLS/SSL и электронную почту.
WSTEP		Протокол Microsoft WS-Trust X.509v3 Token Enrollment Extensions
ИС	Информационная система	
ОС	Операционная система	
ЦС	Центр Сертификации	Центр Сертификации (Certification Authority) — сервер, предназначенный для выпуска и отзыва сертификатов, а также публикации CRL (COC).

Определения

Термин	Определение
Clearway CA	Продукт, информационная система, выполняющая выпуск сертификатов X.509 v3, отзыв сертификатов, формирование CRL/DeltaCRL, предоставление статусов через OCSP, управление шаблонами и прочие операции. Состоит из микросервисов (в т.ч. miniCA), веб-интерфейса, mOCSP, CLI-утилит и др.
miniCA	Наименование основного сервиса/компонента в составе продукта Clearway CA, реализующего ядро выдачи сертификатов. Используется в технических ссылках (код, бинарные артефакты).
Микросервис	Отдельная программа, являющаяся частью программной системы или проекта, реализующая отдельный функциональный или информационный блок и тесно связанная с другими частями системы или проекта через сетевые вызовы API.
Пайплайн (Pipeline)	Последовательность взаимосвязанных этапов, через которые проходят задачи, проекты или данные от начала до завершения.
Плейбук (Playbook)	Формализованный документ или набор инструкций, используемых для автоматизации действий на удалённых машинах. Применяется в инструментах вроде Ansible, содержит перечень задач, необходимых для выполнения определённых операций, и представлен в формате YAML.
Роль	Набор системных и объектных прав/привилегий, присваиваемый субъекту (например: admin, causer, crluser, archuser, jwtadmin), которые могут быть выданы и отозваны как единое целое
Сервер аутентификации	Сервер аутентификации (OIDC / OAuth 2.0) — совместимый с OpenID Connect Core 1.0 (Authorization Code + PKCE), поддерживающий выпуск JWT (RS256/ES256) и JWKS

1. Введение

Настоящий документ относится к эксплуатационной документации ПО «Система централизованного анализа и управления гетерогенными инфраструктурами — Clearway CA» (далее — Clearway CA). Разработчиком Clearway CA является ООО «Клируэй Текнолоджис».

Clearway CA — это центр сертификации, который выполняет выпуск сертификатов X.509v3 на основе CSR-запросов в формате PKCS#10, используя готовые шаблоны. Система позволяет создавать и настраивать эти шаблоны, а также отзыв сертификатов с указанием причины. Clearway CA формирует списки отозванных сертификатов (CRL и DeltaCRL), предоставляет статус сертификатов через протокол OCSP и обеспечивает доступ к ним по серийному номеру или SHA1-отпечатку. Все запросы, сертификаты, журналы событий и CRL/DeltaCRL сохраняются в базе данных. Управление осуществляется через веб-интерфейс Clearway CA и API, а также поддерживается работа с протоколом SCEP для выпуска сертификатов.

Clearway CA является развитием одного из модулей ПО «Система централизованного анализа и управления гетерогенными инфраструктурами (ЦУГИ)», зарегистрированной в Реестре российского ПО (Реестровая запись №13033 от 21.03.2022), обладает расширенным составом функций и позволяет применяться в отдельно устанавливаемом исполнении.

2. Функции Clearway CA

Основной функцией Clearway CA является управление жизненным циклом сертификатов:

- 1) Выпуск сертификатов:
 - Выпуск сертификатов X.509v3 на основе CSR запросов в формате PKCS#10;
 - Поддержка шаблонов сертификатов для заполнения и контроля атрибутов сертификатов;
 - Поддержка выпуска сертификатов по различным протоколам – SCEP, WSTEP и т.п.
- 2) Предоставление сертификата по запросу:
 - Возможность получения выпущенных сертификатов по запросу;
 - Возможность получения различных выборок и отчетов о выпущенных сертификатах.
- 3) Отзыв сертификата:
 - Отзыв сертификатов с указанием причины;
 - Формирование Списка Отозванных Сертификатов (COC, CRL);
 - Формирование разностных списков отозванных сертификатов DeltaCRL;
 - Предоставление информации о статусе сертификата по протоколу OCSP.
- 4) Вспомогательные функции:
 - Сохранение информации о всех запросах, сертификатах, CRL/DeltaCRL в базе данных;
 - Текстовый журнал событий;
 - Поддержка функций самодиагностики;
 - Поддержка хранения ключа ЦС на аппаратных носителях HSM.

3. Логическая архитектура системы

3.1. Программные компоненты системы

Clearway CA реализует автономный многопоточный HTTP сервер с возможностями установления TLS или mTLS (mutual TLS) в зависимости от параметров конфигурации. Сервис эксплуатирует утилиту OpenSSL для выполнения всех криптографических операций, а также операций с различными контейнерами ASN.1 (CSR запросы PKCS#10, сертификаты X.509v3, CRL/DeltaCRL).

Clearway CA построено на базе модульных компонентов, написанных на языках программирования C# (.Net 8.0.x) и Go (1.21 и выше).

В таблице ниже приведено описание функций компонентов.

Таблица 1 — Компоненты Clearway CA и их функции

Компонент	Тип	Необходимые сторонние компоненты	Конфигурационный файл	Функции
miniCA	сервис (демон)	PostgreSQL, OpenSSL	minica.yml	Обеспечивает выполнение всех необходимых функций по управлению жизненным циклом сертификатов.
mclient	консольное приложение		mclient.yml	Внутреннее клиентское приложение для вызова функций Clearway CA с использованием интерфейса командной строки.
mOCSP	сервис (демон)		mocsp.yml	Реализация сервиса OCSP с предоставлением статуса сертификатов в реальном времени.
Веб-интерфейс (контрольная панель)	сервис (демон)	Nginx, KeyCloak	itc_Api_MiniCA_control Panel_config.json	Обеспечение основных функций по управлению сертификатами через графический интерфейс пользователя.
uSCEP	сервис (демон)		uscep.yml	Обеспечивает интерфейс для запроса сертификатов по протоколу SCEP.

Общая схема архитектуры Clearway CA приведена на Рисунок 1.

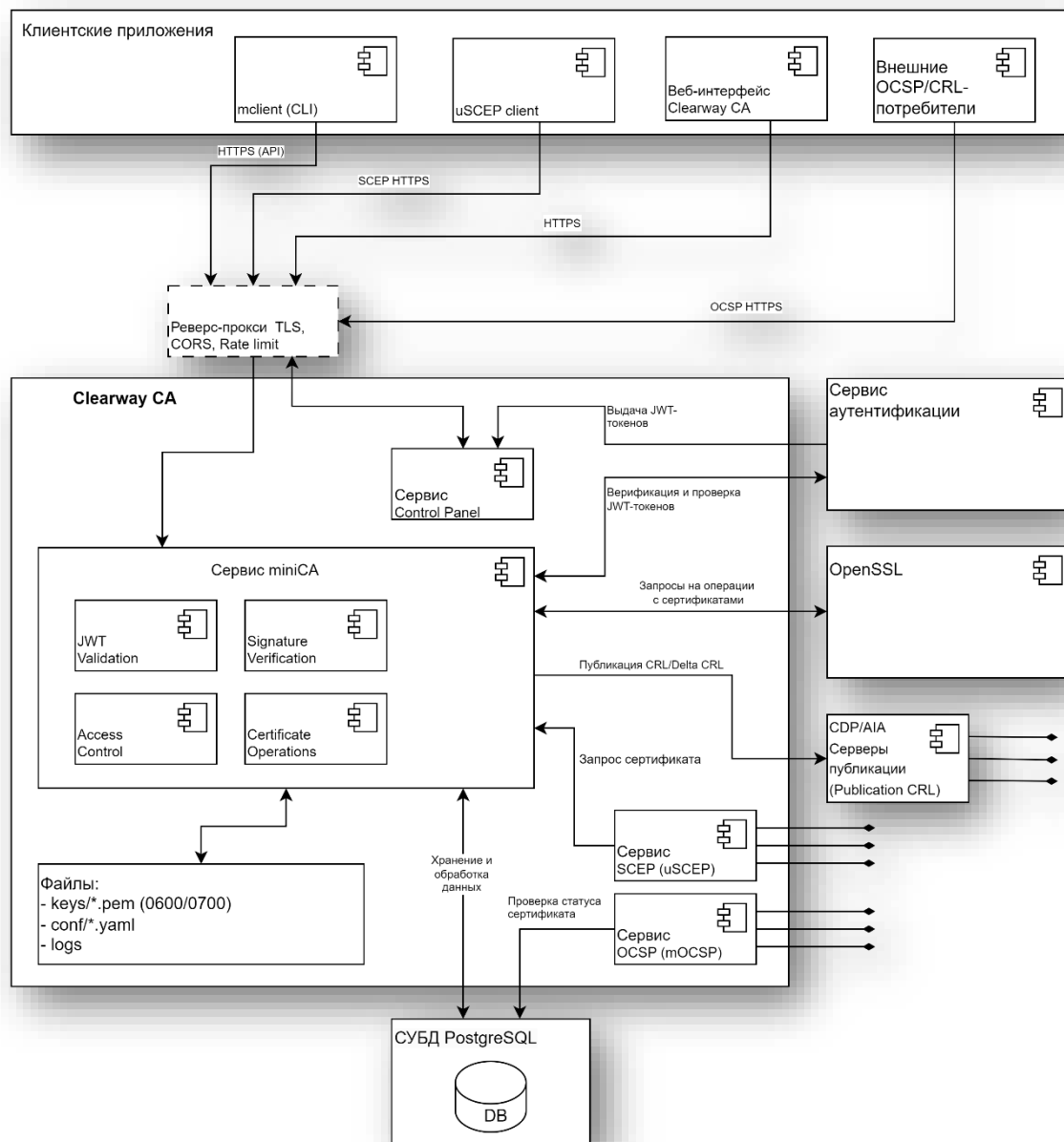


Рисунок 1 — Архитектурная схема Clearway CA

Также в составе Clearway CA имеется ряд дополнительных программных компонентов, расширяющих его возможности.

Микросервис miniCA реализует программный интерфейс с использованием протокола HTTP (или HTTPS). Основные функции микросервиса:

- выпуск сертификатов X.509v3 на основе CSR запросов в формате PKCS#10;
- отзыв сертификатов в соответствии с заданной причиной;

- формирование списка отозванных сертификатов CRL (RFC 5280);
- формирование разностных списков отозванных сертификатов DeltaCRL;
- предоставление информации о статусе сертификата;
- предоставление сертификатов по их серийному номеру или SHA1 отпечатку;
- сохранение информации о всех запросах, сертификатах, CRL/DeltaCRL и журнала событий в базе данных.

Протокол информационного взаимодействия между сервисом и клиентом основан на передаче структур данных JSON (запрос → ответ). Все запросы к микросервису должны быть подписаны закрытым ключом, известным только клиенту. Открытый ключ для проверки подписи запросов сервис извлекает из X.509v3 сертификата, заданного конфигурацией. Опционально проверка подписи может быть отключена.

На время выполнения операций с OpenSSL применяется блокировка (мьютекс). Система может быть масштабирована использованием нескольких микросервисов ClearwayCA, работающих параллельно с одной базой данных.

Операционная система — GNU/Linux. Целевая система Astra Linux SE 1.7 «Воронеж». Возможна эксплуатация с использованием других распространенных дистрибутивов ОС Linux (Debian/Ubuntu/Fedora) и их производных. При необходимости микросервис может быть запущен в контейнере docker (podman).

3.2. Описание архитектуры Clearway CA

Дистрибутив Clearway CA включает следующие исполняемые компоненты:

- miniCA — основной сервис (API) Центра Сертификации: выпуск и отзыв сертификатов, формирование/выдача CRL и DeltaCRL, операции поиска/экспорта, управление шаблонами сертификатов, операции с JWT, ведение журналов.
- mOSCP — сервис проверки статуса сертификатов (OCSP-responder) с кешированием ответов и поддержкой GET/POST (DER).
- Веб-интерфейс Clearway CA (Control Panel) — компонент управления и операционной работы через браузер; использует API сервиса minica и реализует аутентификацию по JWT и ролевое разграничение доступа.
- CLI-утилиты: mclient (вызов API из командной строки), mjwt (операции с JWT и ключами подписи), signer (вспомогательные крипто-операции/подпись), grpsql (диагностика/администрирование БД), maskpass (скрытый ввод секретов).

Для управления конфигурацией сервиса miniCA используется файл minica.yml (YAML). Путь к конфигурации может задаваться параметром запуска или переменной окружения MINICA_CONF. Для секретов и транспорта используются переменные окружения (например: MINICA_PASS,

JWT_KEY/JWT_KEYS, TLS_CERT/TLS_KEY/TLS_CA_CERT, CHAIN_FILE и др.). Логирование поддерживает ротацию и маскирование чувствительных данных.

Политика выпуска сертификатов. Параметры X.509 v3 определяются шаблонами (хранятся в БД) в сочетании с конфигурацией openssl.cnf: в шаблоне задаются основные атрибуты (BC/KU/EKU/SAN и др.) и ссылка на соответствующую секцию расширений в openssl.cnf. Выпуск выполняется на основе указанного шаблона и правил OpenSSL.

В качестве СУБД используется PostgreSQL. СУБД может быть локальной или вынесенной на отдельный сервер/кластер. Реквизиты подключения задаются в конфигурации, для защищённых развёртываний применяется TLS с проверкой подлинности сервера (рекомендуется режим verify-full).

Сервисы предназначены для работы под управлением Linux, рекомендуется запуск через systemd. Внешние взаимодействия API и OCSP работают по HTTP(S), для защищённых контуров включается TLS/mTLS согласно настройкам. Control Panel разворачивается вместе с серверной частью и обращается к API miniCA внутри доверенного сегмента либо через защищённый периметр.

3.3. Описание архитектуры веб-интерфейса Clearway CA

Веб-интерфейс Clearway CA (далее Control Panel) — компонент Clearway CA, обеспечивающий доступ к функциям управления через веб-браузер. Control Panel предназначен для доступа к функциям выдающего ЦС, а также размещения CDP, OCSP и прочих компонентов.

Control Panel состоит из двух пакетов и одной исполняемой программы:

- miniCA-cp-service — приложение микросервиса;
- miniCA-spa — интерфейс приложения и конфигурационные файлы.
- Микросервис также использует программу Nginx для перенаправления веб-интерфейса.

Для автоматизации запуска микросервиса рекомендуется применение службы `systemd`, входящей в большинство современных дистрибутивов Linux.

В качестве СУБД используется PostgreSQL. Реквизиты доступа к базе данных указываются в параметрах конфигурации.

Конфигурация микросервиса описывается в конфигурационном файле в формате JSON. Некоторые опции могут быть заданы опциями командной строки (путь к конфигурационному файлу, опции журнала). Диаграмма взаимодействия программных компонентов приведена на Рисунок 2.

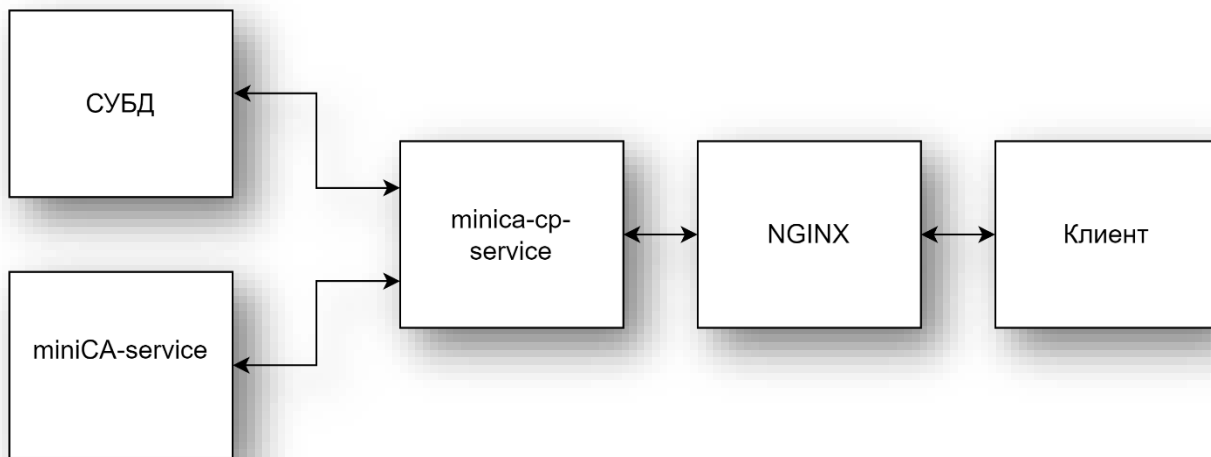


Рисунок 2 — Диаграмма взаимодействия программных компонентов веб-интерфейса Clearway CA

3.4. Описание архитектуры mOSCP

МОСРП специализированный микросервис для быстрой онлайн-проверки текущего статуса цифровых сертификатов, используемый в инфраструктуре открытых ключей (PKI). Состоит из одного пакета и одной исполняемой программы:

- mosp — приложение микросервиса;

Для автоматизации запуска микросервиса рекомендуется применение службы `systemd`, входящей в большинство современных дистрибутивов Linux.

В качестве СУБД используется PostgreSQL. Реквизиты доступа к базе данных указываются в параметрах конфигурации.

Конфигурация микросервиса описывается в конфигурационном файле в формате JSON. Некоторые опции могут быть заданы опциями командной строки (путь к конфигурационному файлу, опции журнала). Диаграмма взаимодействия программных компонентов приведена на Рисунок 3.

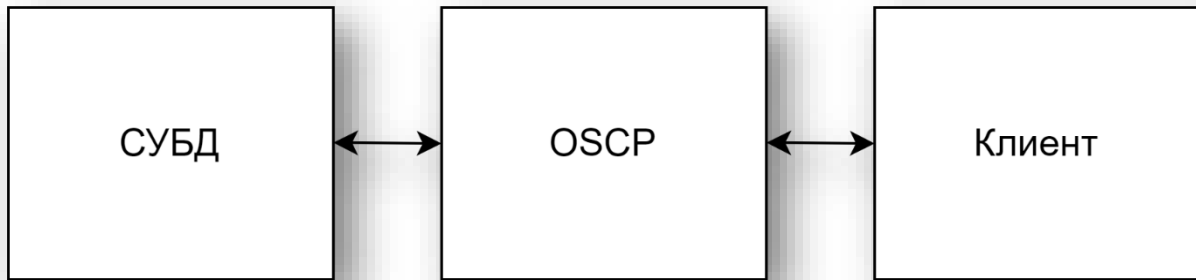


Рисунок 3 — Диаграмма взаимодействия программных компонентов MOSCP

3.5. Сторонние программные компоненты

Все программные компоненты ClearwayCA протестированы на следующих операционных системах:

- Astra Linux 1.7.4 и выше;
- Debian 12.

Для работы ClearwayCA используется база данных PostgreSQL версии 15 и выше.

Для работы веб-консоли необходим Nginx версии 1.26.0 и выше.

3.6. Алгоритм типовой операции

ClearwayCA работает как веб-сервис и принимает на вход HTTP-запрос. При этом выполняется ряд проверок. Ниже приведен порядок обработки типового запроса к ClearwayCA:

- 1) Клиент отправляет HTTP-запрос на сервис miniCA. Запрос содержит два компонента: данные в виде base64-кода и цифровую подпись этих данных.
- 2) Микросервис проверяет заголовок Authorization, где содержится JWT-токен. Проверяется:
 - 1) Алгоритм подписи токена (HS256, RS256, ES256 или EdDSA);
 - 2) Значения полей `iss` и `sub`:
 - `iss` содержит уникальный идентификатор ключа сервера;
 - `sub` содержит идентификатор открытого ключа клиента.
- 3) После успешной проверки токена, микросервис декодирует данные и цифру (`signature`) из запроса. Данные представляют собой JSON-объект, закодированный в base64.

- 4) Проверяется цифровая подпись данных — miniCA вычисляет SHA-256-хеш распакованного JSON-объекта и сравнивает его с цифровой подписью, приложенной клиентом.
- 5) Если подпись совпадает, проходит дополнительная проверка прав доступа клиента, исходя из ролевой модели или списка разрешенных операций.
- 6) Производится непосредственное выполнение запрошенной операции с сертификатами: создание, обновление, аннулирование и т.п.
- 7) Применяется блокировка (мьютекс) для исключения возможных проблем параллельного доступа к общим данным (конфликты записи/чтения) и предотвращения ситуации, когда разные потоки одновременно пытаются изменить одни и те же ресурсы.
- 8) Результат выполненной операции сохраняется в базе данных PostgreSQL.
- 9) Формируется ответ клиенту. Ответ состоит из двух частей:
 - Основной объект данных (результат операции), закодированный в base64;
 - Новая цифровая подпись этого объекта, созданная сервером.
- 10) Ответ отправляется клиенту, завершая весь цикл обработки запроса.

4. Физическая архитектура

4.1. Типовые конфигурации

Физическая архитектура включает следующие узлы (серверы/виртуальные машины), на которых развернуты сервисы и компоненты Clearway CA:

- Узлы сервисов ЦС — размещение микросервиса miniCA (ядро API и операции с сертификатами);
- Узел/кластер СУБД PostgreSQL — хранение запросов, сертификатов, CRL и журналов.
- Узлы публикации CDP/AIA — веб-/файловые серверы для размещения CRL и цепочек сертификатов;
- Узел веб-интерфейса (Control Panel / UI) — сервер приложений для административного доступа через браузер;
- Узлы SCEP (uSCEP) — обработка SCEP-запросов от устройств (при использовании);
- Узлы OCSP (mOCSP) — обработка OCSP-запросов статуса сертификатов (публичная точка по конфигурации).

Все компоненты могут размещаться на отдельных серверах или совмещаться в произвольном сочетании.

Существует несколько типовых конфигураций, рекомендуемых для развертывания в инфраструктурах организаций. Типовые конфигурации приведены в Таблица 2

Таблица 2 — Типовые конфигурации

Название	Список серверов	Рекомендация к установке
Базовая установка, 1 сервер	Все компоненты Clearway CA и СУБД PostgreSQL размещаются на одном сервере	Рекомендуется для тестовых стендов или инфраструктур с небольшой нагрузкой на ЦС без высоких требований к доступности.
Типовая, без отказоустойчивости, 2 сервера	<ul style="list-style-type: none"> – Сервер Clearway CA: сервисы ЦС, сервис CDP&AIA, сервис OCSP, веб-сервер, сервис SCEP; – Сервер PostgreSQL 	<p>Описанная конфигурация обладает высокой производительностью, но не обеспечивает отказоустойчивости. Рекомендуется для ЦС без высоких требований к доступности.</p> <p>Допускается размещение компонентов Clearway CA как на одном сервере, так</p>

Название	Список серверов	Рекомендация к установке
		и на нескольких серверах (см. Рисунок 5)
Распределенная, с отказоустойчивостью	<ul style="list-style-type: none"> – 2 или более серверов Clearway CA: сервисы ЦС; – 2 или более серверов CDP&AIA + OCSP; – 1 или 2 сервера Веб-консоли; – 1 или более серверов SCEP (при необходимости); – Кластер PostgreSQL. 	Рекомендуется для высоконагруженных ЦС, имеющих высокие требования к отказоустойчивости.

В Таблица 3 ниже приведен список межкомпонентных взаимодействий и требуемых портов.

Таблица 3 — Информационные потоки Clearway CA

№	Инициатор	Получатель	Протокол	Порт по умолчанию	Описание
1)	Сервер Clearway CA	Сервер PostgreSQL	TCP	5432	Чтение и запись данных
2)	Веб сервер точек распространения	Сервер Clearway CA	HTTPS	443	Получение CRL
3)	SCEP	Сервер Clearway CA	HTTPS	443	Запрос сертификатов
4)	Control Panel	Сервер Clearway CA	HTTPS	443	Запрос сертификатов, настройка ЦС и шаблонов
5)	Control Panel	Сервер PostgreSQL	TCP	5432	Получение списка сертификатов
6)	OCSP	Сервер PostgreSQL	TCP	5432	Чтение данных о сертификатах
7)	Драйвер ЦС	Сервер Clearway CA	HTTPS	443	Запросы на выпуск сертификатов
8)	Все потребители	Веб сервер точек распространения и OCSP	HTTP	80	Доступ пользователей к AIA, CDP, OCSP
9)	Клиенты SCEP	SCEP	HTTPS	443	Запрос сертификатов
10)	APM администратора	Все серверы компонентов Clearway CA	SSH	22	Доступ администраторов для настройки и аудита

Схемы инфраструктуры для развертывания Clearway CA приведены на рисунках ниже.

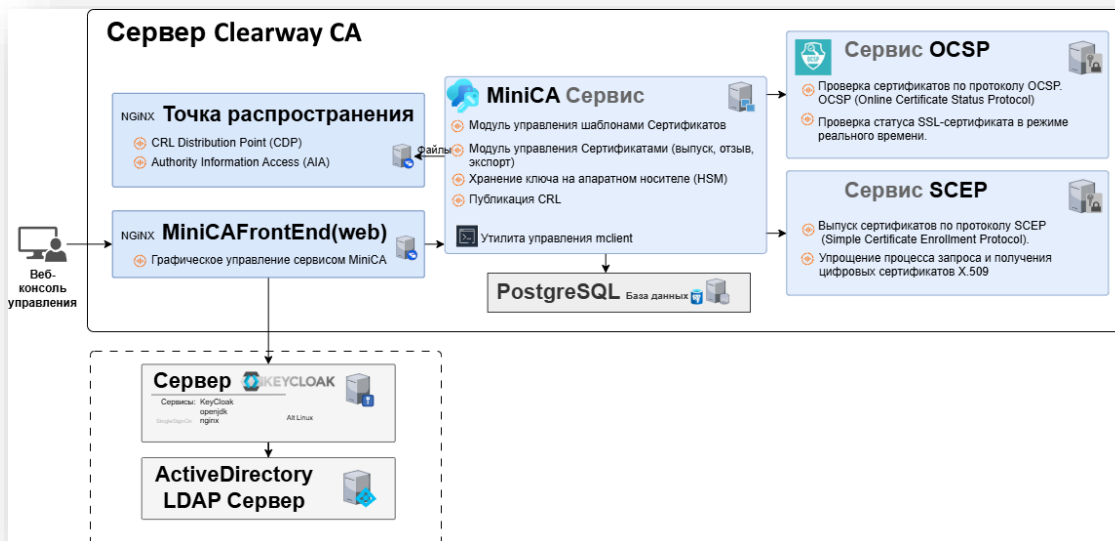


Рисунок 4 — Базовая схема ИТ-инфраструктуры.

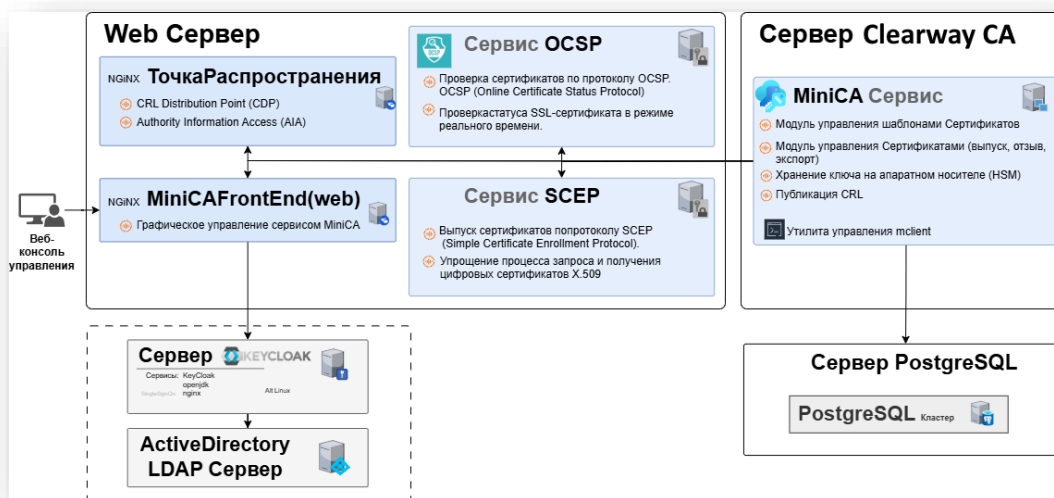


Рисунок 5 — Типовая (рекомендуемая) схема ИТ-инфраструктуры.

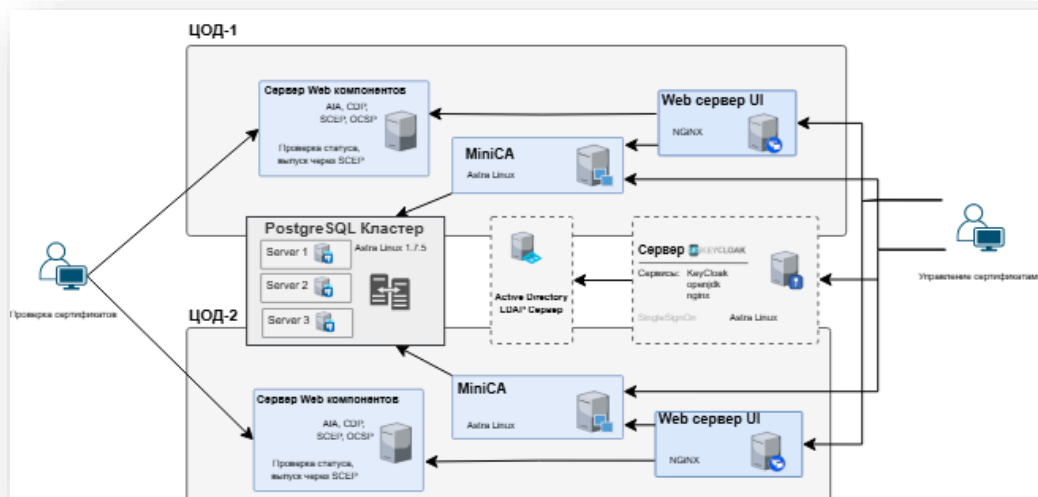


Рисунок 6 — Распределенная схема ИТ-инфраструктуры

4.2. Технические требования

4.2.1. Рекомендуемые технические требования к серверному оборудованию

Таблица 4 — Аппаратные требования к минимальной конфигурации

№	Наименование ТС	Кол-во серверов	CPU, кол-во ядер	CPU, тактовая частота, не менее, ГГц	RAM, Гб	SSD, Гб	ОС	Описание
1)	Сервер Clearway CA + Control panel + СУБД PostgreSQL	1	4	2	4	256	Astra Linux 1.7.5 Orel	Включает поли PostgreSQL, Control Panel, AIA, CDP и OCSP. Рекомендации по применению: корневой ЦС, выдающий ЦС для небольших организаций (до 100 сертификатов в сутки).

Таблица 5 — Рекомендуемые аппаратные требования к базовой конфигурации

№	Наименование ТС	Кол-во серверов	CPU, кол-во ядер	CPU, тактовая частота, не менее, ГГц	RAM, Гб	SSD, Гб	ОС	Описание
2)	Сервер Clearway CA + Control panel + СУБД PostgreSQL	1	4	2	8	512	Astra Linux 1.7.5 Orel	Включает поли PostgreSQL, Control Panel, AIA, CDP и OCSP. Рекомендации по применению: выдающий ЦС для организаций со средней нагрузкой (до 5000 сертификатов в сутки).

Таблица 6 — Рекомендуемые аппаратные требования к типовой конфигурации

№	Наименование ТС	Кол-во серверов ¹	CPU, кол-во ядер	CPU, тактовая частота, не менее, ГГц	RAM, Гб	SSD, Гб	ОС	Описание
1)	Сервер Clearway CA	1 или 2	8	2	16	256	Astra Linux 1.7.5 Orel	Основной сервер Clearway CA. Рекомендации по применению: выдающий ЦС, для высоконагруженных систем, с использованием K8S, service mesh
2)	Сервер СУБД PostgreSQL	1 или кластер СУБД	4	2	8	512	Astra Linux 1.7.5 Orel	Сервер PostgreSQL
3)	Сервер control panel	1 или 2	2	2	4	100	Astra Linux 1.7.5 Orel	Control Panel, AIA, CDP и OCSP

¹ 2 сервера используются для распределения нагрузки и обеспечения отказоустойчивой работы компонентов Clearway CA

4.2.2. Требования к АРМ оператора

Таблица 7 — Требования к АРМ оператора

№	Требования к ПК для рабочих мест	Ядер	Тактовая частота не менее, ГГц	RAM, ГБ	SSD, ГБ	Браузер	Операционная система
1)	АРМ оператора	2	2	4	80	Google Chrome версия не ниже 113, браузеры на Chromium (Microsoft Edge, Яндекс.Браузер).	Windows 10+

4.2.3. Требования к системному ПО

Таблица 8 — Требования к системному ПО

Сервер / АРМ, на который устанавливается ПО	Наименование ПО	Минимальная версия	Рекомендуемая версия	Назначение
Сервер control panel	dot.Net	8.0	8.0	Компонент системы
	nginx	Установка из репозитория		Веб сервер
	curl	Установка из репозитория		Обращение к API системы
	jq	Установка из репозитория		Для скрипта формирования токена для обращения к API
Сервер Clearway CA	psql	Установка из репозитория	Не ниже версии БД	Для создания БД и таблиц
Сервер аутентификации (пример конфигурации)	KeyCloak	19.0.3	24.0.2 и выше	Авторизация
	openjdk	11 (зависит от версии Keycloak)	17 (зависит от версии Keycloak)	Для работы keycloak

Сервер / АРМ, на который устанавливается ПО	Наименование ПО	Минимальная версия	Рекомендуемая версия	Назначение
	nginx	Установка из репозитория		Веб сервер
Сервер СУБД	PostgreSQL	11	15	База данных
	etcd	Установка из репозитория		Обеспечение работы кластера PostgreSQL
	patroni	Установка из репозитория		Обеспечение работы кластера PostgreSQL
АРМ администратора	Dbeaver +pg_utils(pg_dump, pg_dumpall, pg_restore, psql) +driver PostgreSQL	21.3.1	Самая последняя	Для настройки и эксплуатации БД
	WinSCP	5.13.7	Самая последняя	Доступ к файлам серверов
	putty	0.70	Самая последняя	Доступ к серверам по ssh
	liquibase	4.7.1	Самая последняя	Первичное наполнение/обновление БД
	Google Chrome	113	Самая последняя	Доступ к веб интерфейсу системы

4.2.4. Требование к сети

Источник	Назначение	Порты	Описание
АРМы (операторов, администраторов, пользователей и т.д)	Clearway CA сервер, сервер панели управления, Keycloak сервер	443	Доступ к Веб-консоли Системы

Источник	Назначение	Порты	Описание
Сервер Control Panel, Keycloak сервер	Контроллеры домена	389,636	Доступ к AD для чтения пользователей, авторизации
APM администратора	Сервер панели управления, Keycloak сервер	22,443	Доступ для настройки и сопровождения
APM администратора	Сервер БД	5432 (или порты, выделенные для данного подключения)	Доступ для настройки и сопровождения

4.2.5. Требования к учётным записям

Название	Расположение	Права	Описание
ltc-mca-svc	Домен	Active Directory: чтение Центры сертификации Microsoft: чтение ЦС, запуск в качестве задания	Доступ к Active Directory на чтение (обычная УЗ без каких-либо прав) Чтение сертификатов для импорта в Clearway CA
ltc-mca-mail	Доменная (или иная – зависит от почтовой системы)	Отрывка почтовых уведомлений	УЗ с правом отправлять почтовые уведомления
ltc-svc	Локальная Clearway CA сервер	Запуск служб Домашняя папка Запуск crontab Папка /app (RW)	Локальная УЗ для запуска служб системы
keycloak	Локальная, Keycloak сервер	Запуск служб Домашняя папка Запуск crontab Папка /app (RW)	Локальная УЗ для запуска службы Keycloak

Название	Расположение	Права	Описание
ltc-svc	Локальная БД сервер	БД owner: Clearway CA	Локальная УЗ для доступа к БД
УЗ администратора	Доменная	APM администратора: RDP Clearway CA сервер: ssh, root или переключение в контекст ltc-svc, nginx(www-data) Keycloak сервер: ssh, root или переключение в контекст keycloak	УЗ для доступа к серверам

4.2.6. Группы

Имя	Тип	Описание
ITC_MCA_Administrators	Доменная	Администраторы инфраструктуры
ITC_MCA_Operators	Доменная	Операторы
ITC_MCA_Auditors	Доменная	Аудиторы

4.2.7. Дополнительно

Для нормальной работы сертификатов, выданных Clearway CA, необходимо внести сертификат Clearway CA в контейнеры TrustedRoot на серверах и АРМ.

Предпочтительны права Root на серверах для развёртывания системы.

5. Обеспечение безопасности

5.1. Защита ключа ЦС

В таблице ниже описаны варианты хранения ключа ЦС и меры по обеспечению его безопасности.

Таблица 9 — Варианты хранения ключа ЦС и меры по обеспечению его безопасности

Способ хранения	Методы защиты	Примечание
При помощи аппаратных устройств HSM	Ключ внутри HSM не может быть извлечен, поэтому защита сводится к ограничению доступа пользователей к интерфейсу HSM.	
На файловой системе	<ul style="list-style-type: none">Разрешение на чтение ключа имеет только технологическая учётная запись, от которой запущен Clearway CA;Шифрование файла ключа.	В случае шифрования файла ключа при запуске Clearway CA должен быть введен ключ шифрования.

5.2. Защита файлов системы

Исполняемые, конфигурационные и вспомогательные файлы компонентов Clearway CA защищены при помощи разрешений операционной системы:

- Владельцем файлов и папок является технологическая учётная запись, от которой запускается Clearway CA;
- На файлы и папки установлены разрешения 700.

5.3. Защита БД

Для защиты базы данных Clearway CA должны быть предприняты следующие меры:

- Владельцем БД Clearway CA является учётная запись, от имени которой происходит взаимодействие Clearway CA и PostgreSQL;
- Для чтения БД выделяется отдельная учетная запись с доступом только для чтения;
- В случае хранения в БД чувствительной информации (например, при использовании KRA), она хранится в зашифрованном виде.

5.4. Защита сетевых взаимодействий

Все взаимодействия между компонентами системы, а также между компонентами и пользователями, защищены при помощи TLS. Также возможна настройка mTLS.

5.5. Ролевая модель

Контроль доступа пользователей к функциям ЦС является важнейшим элементом безопасности всей информационной инфраструктуры организации. Clearway CA имеет продвинутую систему разделения полномочий пользователей на разных уровнях.

В разделах ниже описана реализация ролевой модели для Clearway CA и Веб-консоли управления.

5.5.1. Ролевая модель, Control Panel

Аутентификация и авторизация в графическом Веб-консоли осуществляется при помощи сервера аутентификации (OIDC / OAuth 2.0), совместимого с OpenID Connect Core 1.0 (Authorization Code + PKCE) и поддерживающего выпуск JWT (RS256/ES256) и JWKS), и службы каталогов, в частности, Microsoft Active Directory. В качестве сервера аутентификации может использоваться Keycloak, Dex или эквивалент.

Роли пользователя присваиваются группам AD в консоли администрирования сервера аутентификации. Для получения соответствующей роли учетная запись пользователя должна быть добавлена в ролевую группу AD. В составе токена аутентификации Control Panel получает роль пользователя и предоставляет разрешенные в соответствии с ролью элементы управления.

Реализованы следующие роли пользователей:

- Администратор ЦС;
- Менеджер сертификатов;
- Аудитор;
- Пользователь.

Роль "Пользователь" предоставляется всем пользователям по умолчанию и может быть совмещена с другими ролями. В таблице указана доступность функций системы для каждой роли.

Таблица 10 — Роли Clearway CA

Наименование роли	Описание доступных действий и полномочий
Администратор	— Изменение настроек и параметров ЦС;

Наименование роли	Описание доступных действий и полномочий
	– Настройка шаблонов.
Аудитор	– Просмотр журналов событий, отчётов. – Просмотр конфигурации ИС.
Менеджер сертификатов	– Отзыв сертификатов; – Публикация CRL.
Пользователь	– Доступ на чтение к информации CDP&AIA; – Формирование запросов на сертификаты.

5.5.2. Ролевая модель Clearway CA

Ниже описана реализация ролевой модели Clearway CA на основе подписи запросов и JWT-токенов.

Она построена на проверке и обработке JSON Web Token (JWT), обеспечивающих управление доступом и контроль над функциональностью клиентского приложения. Конфигурируется блок JWT, включающий следующие параметры:

Таблица 11 — Параметры блока JWT

Параметр	Описание	Пример
<code>no-check</code>	Логический переключатель, управляющий проверкой JWT-токенов. Если установлен в true, проверка токенов отключается, однако остается доступна проверка подписанных запросов главным ключом.	<code>no-check: false</code>
<code>key</code>	Файл с приватным ключом для подписи JWT-токенов, расположенный в папке conf. Формат файла — PEM.	<code>key: "conf/jwt.key"</code>
<code>keys</code>	Каталог с файлами ключей для проверки JWT-токенов. Названия файлов формируются по стандарту SKI (Subject Key Identifier) и имеют формат XX...XX.PEM.	<code>keys: "conf/jwt-keys"</code>
<code>cache-minutes</code>	Время хранения ключей в кэше (в минутах).	<code>cache-minutes: 5</code>

Параметр	Описание	Пример
<code>roles</code>	Перечень ролевых моделей и назначаемых им прав. Каждый профиль имеет свою область ответственности и функциональные возможности.	Подробнее в таблице Таблица 12 — Описание ролей JWT.
<code>sign-off</code>	Логическая опция отключения проверки подписи запросов. При значении true проверка подписей также отключается.	<code>sign-off: false</code>
<code>master-key</code>	Файл с главным ключом проверки подписи запросов. Обычно является открытым ключом или HMAC-секретом.	<code>master-key: "conf/mclient.pem"</code>
<code>chain-file</code>	Файл с цепочкой сертификатов (PEM-формат).	<code>chain-file: "ca/ca-chain.pem"</code>

Таблица 12 — Описание ролей JWT

Роль	Наименование	Описание	Права
admin	Администратор	Возможность просмотра статуса системы, выдачи сертификатов, обновления списков отмены, восстановления повреждённых записей и управления JWT-токенами.	<ul style="list-style-type: none"> – ping; – ca; – revoke; – status; – get; – updctrl; – ctrl; – updeltctrl; – deltacrl; – find; – delete; – export; – templates; – csr; – repair; – stat; – gettempl; – addtempl; – deltempl;

Роль	Наименование	Описание	Права
			<ul style="list-style-type: none"> – mkjwt; – revokejwt; – repairjwt; – deljwt; – getjwt; – renewjwt; – revivejwt; – chain.
causer	Центр регистрации	Доступ к функционалу центра сертификации (выпуск, отзыв, статус, восстановление сертификатов).	<ul style="list-style-type: none"> – ping; – ca; – revoke; – status; – get; – repair; – csr; – templates; – gettempl; – chain.
crluser	Пользователь списка аннулирования	Обновление и получение списков отзыва сертификатов (CRL и DeltaCRL).	<ul style="list-style-type: none"> – ping; – updcrll; – crl; – updeltacrll; – deltacrll; – chain.
archuser	Архивариус	Удаление ненужных записей из базы данных.	<ul style="list-style-type: none"> – ping; – status; – get; – crl; – deltacrll; – find; – delete; – export; – templates; – stat; – gettempl; – csr;

Роль	Наименование	Описание	Права
			– getjwt.
exporter	Экспортёр	Экспорт данных из хранилища.	<ul style="list-style-type: none"> – ping; – status; – get; – crl; – deltacrl; – find; – export; – templates; – stat; – gettempl; – csr; – getjwt.
templadmin	Администратор шаблонов	Управление шаблонами сертификата.	<ul style="list-style-type: none"> – ping; – templates; – gettempl; – addtenpl; – deltempl.
jwtadmin	Администратор JWT	Полный доступ к управлению JWT-токенами (выдача, отзыв, восстановление, удаление).	<ul style="list-style-type: none"> – ping; – mkjwt; – revokejwt; – repairjwt; – getjwt; – deljwt; – revivejwt.

В таблице ниже описаны операции Clearway CA.

Каждой операции соответствует отдельная команда сервиса MiniCA.

Таблица 13 — Описание операций

Операция	Пояснение
ping	Проверка доступности службы
ca	Управление центром сертификации
revoke	Отзыв выданных сертификатов
status	Мониторинг текущего состояния системы

Операция	Пояснение
<code>get</code>	Получение данных
<code>updcrl</code>	Обновление основных списков отозванных сертификатов
<code>crl</code>	Получение списков отозванных сертификатов
<code>updelcrl</code>	Обновление инкрементальных списков отозванных сертификатов
<code>deltacrl</code>	Получение частичных списков отозванных сертификатов
<code>find</code>	Поиск данных в системе
<code>delete</code>	Удаление ресурсов
<code>export</code>	Экспорт информации
<code>templates</code>	Управление шаблонами сертификатов
<code>csr</code>	Обработка запросов на сертификаты (CSR-запросы)
<code>repair</code>	Исправление ошибок в системе
<code>stat</code>	Получение статистики
<code>gettempl</code>	Получение существующих шаблонов сертификатов.
<code>addtempl</code>	Добавление новых шаблонов сертификатов.
<code>deltempl</code>	Удаление шаблонов сертификатов.
<code>mkjwt</code>	Создание новых JWT-токенов
<code>revokejwt</code>	Отзыв действующих JWT-токенов
<code>repairjwt</code>	Восстановление JWT-токенов
<code>deljwt</code>	Принудительное удаление JWT-токенов
<code>getjwt</code>	Получение сведений о JWT-токене
<code>renewjwt</code>	Продление срока действия JWT-токена
<code>revivejwt</code>	Возобновление временного блокировки JWT-токена
<code>chain</code>	Управление цепочками сертификатов