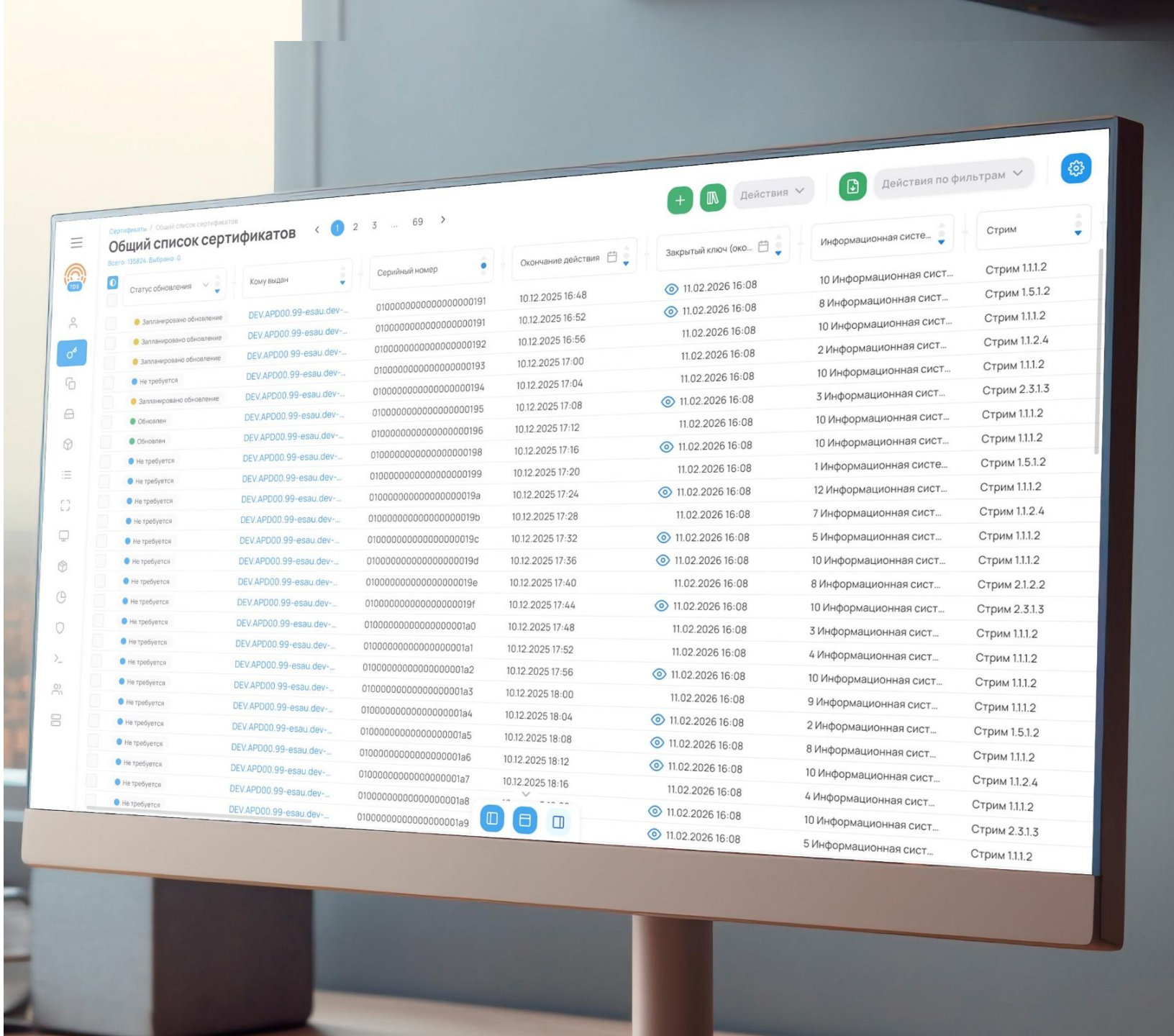
CLEARWAY INTEGRATION

Clearway CA

Алексей Глабец

Владелец продукта



Что такое цифровой сертификат

CLEARWAY INTEGRATION

Определение

Сертификат X.509 — это цифровой документ (криптографический стандарт), который связывает открытый ключ с владельцем (субъектом) с помощью цифровой подписи удостоверяющего центра (CA);

Основное назначение

Подтверждение подлинности веб-сайтов (TLS/SSL), серверов, клиентов и устройств, обеспечение шифрования и целостности данных;

Из чего состоит

Содержит версию, серийный номер, алгоритм подписи, издателя (CA), срок действия, субъекта (владельца), открытый ключ субъекта и уникальные идентификаторы;

Как заверяется

CA добавляет свою цифровую подпись (хэш содержимого сертификата, зашифрованный закрытым ключом CA), что гарантирует неизменность подписанного сертификата;

Как работает (на примере TLS)

- Сервер отправляет клиенту свой X.509-сертификат;
- Клиент проверяет подпись CA, срок действия и имя хоста;
- Убедившись, клиент использует открытый ключ из сертификата для шифрования сеансового ключа.

Примеры использования сертификатов

CLEARWAY INTEGRATION

Защита каналов связи (TLS/SSL)

- Обеспечение конфиденциальности и целостности данных при передаче по открытым сетям.
- Аутентификация серверов и клиентов (взаимная аутентификация).
- Примеры: HTTPS, Wi-Fi и VPN-соединения, защита API-шлюзов.

Электронная подпись (ЭП)

- Подтверждение авторства и целостности электронных документов.
- Неотрекаемость (non-repudiation) - свойство ИБ, означающее, что сторона, подписавшая документ, не может позже отрицать этот факт.
- Примеры: подписание договоров, финансовых документов, отчётности, внутренних распорядительных актов.

Защита ПДн и конфиденциальной информации

- Шифрование данных при хранении и передаче в соответствии с 152-ФЗ и отраслевыми стандартами.
- Обеспечение невозможности восстановления данных при утечке носителей.
- Примеры: защита баз данных, файловых хранилищ, электронной почты, резервных копий.

Аутентификация и управление доступом

- Использование сертификатов для подтверждения личности пользователей и устройств.
- Реализация однофакторной и двухфакторной аутентификации на корпоративных порталах и в системах.
- Примеры: вход в веб-приложения, доступ к виртуальным рабочим столам, подключение к корпоративной сети по сертификатам.

Формальные задачи СКЗИ (регуляторные требования)

- Обеспечение контроля целостности ПО, защита от НСД, регистрация криптографических событий.
- Поддержка импортозамещённых алгоритмов (ГОСТ Р 34.10, 34.11, 28147-89).
- Интеграция с системами учета ключей и сертификатов в составе государственных и корпоративных инфраструктур.

Как работает асимметричная криптография

CLEARWAY INTEGRATION

Ключевая пара

Используются два разных, но математически связанных ключа — открытый (public) и закрытый (private). Открытый ключ можно свободно распространять. Закрытый ключ должен храниться в секрете;

Принцип действия

Отправитель шифрует данные открытым ключом получателя. Зашифрованный текст можно расшифровать только соответствующим закрытым ключом получателя;

Цифровая подпись

Отправитель шифрует хэш сообщения своим закрытым ключом - создаёт подпись. Любой желающий может расшифровать хэш с помощью открытого ключа отправителя и тем самым проверить подпись, убеждаясь в подлинности и целостности.

Главное преимущество

Нет необходимости в защищённом канале для передачи ключа (в отличие от симметричной криптографии).

Области применения сертификатов

CLEARWAY INTEGRATION

Сертификаты применяются для аутентификации и шифрования в различных областях, где необходимо подтверждать подлинность сторон взаимодействия, обеспечивать целостность и авторство данных, защищать канал связи.

Аутентификация и идентификация серверов

подтверждение подлинности узлов при установлении защищённого соединения по протоколу TLS;
защита от подмены узла и перехвата трафика;

Аутентификация и идентификация клиентов

проверка подлинности при доступе пользователей и устройств к информационным системам;
вход по сертификату вместо пароля;

Электронная подпись

подтверждение авторства и целостности документов, программного кода, исполняемых файлов;

Шифрование данных

шифрование данных при хранении и передаче, защита электронной почты (стандарт S/MIME);

Назначение CA

CLEARWAY INTEGRATION

Удостоверяющий центр — компонент Инфраструктуры Открытых Ключей, обеспечивающий управление сертификатами на протяжении всего жизненного цикла.

Выпуск сертификатов

процесс проверки подлинности заявителя и формирования цифрового сертификата с подписью Центра Сертификации, удостоверяющего принадлежность открытого ключа заявителю;

Отзыв сертификатов

досрочное прекращение действия сертификата при компрометации, смене атрибутов, выводе из эксплуатации и т.д.;

Публикация статусной информации

формирование и публикация Списков Отозванных Сертификатов (CRL), обеспечение работы протокола оперативной проверки статуса (OCSP);

Поддержание цепочки доверия

построение иерархии «корневой центр → подчинённый центр → конечный субъект» и обеспечение проверяемости пути сертификации;

Соблюдение политик

выпуск сертификатов согласно политике применения и регламенту, контроль профилей и ограничений (назначение ключа, ограничения имён, длина пути сертификации и т.д.).

Архитектура доверия CA

Иерархия удостоверяющего центра и выпуск сертификатов

На слайде представлена иерархия удостоверяющего центра и порядок выпуска сертификатов:

Корневой ЦС

- Является вершиной доверия;
- Имеет самоподписанный сертификат;
- Выпускает сертификаты для подчинённых ЦС;
- Доверие распространяется от корневого ЦС на все подчиненные ЦС;
- Доверие к корневому ЦС обеспечивается явным указанием его сертификата в соответствующих файлах и контейнерах в ОС;
- Доверие к «чужой» PKI могут обеспечивать Cross-сертификаты, подписанные собственным корневым ЦС.

Подчинённый ЦС

- выпускает сертификаты для конечных субъектов используя для подписи сертификат, полученный от корневого ЦС.
- определяет применение политик безопасности для всех нижестоящих УЦ (Policy CA, Qualified Certification)

Конечные субъекты

- серверы, пользователи, устройства и сервисы — получают сертификаты от подчинённого ЦС и являются завершающим звеном цепочки выпуска.

Почему возникла потребность

CLEARWAY INTEGRATION

1

Импортозамещение зарубежных решений

В условиях санкционных рисков и прекращения официальной поддержки зарубежных вендоров возникает необходимость замены иностранного ПО на альтернативные решения.

2

Требования регуляторов

Требования регуляторов к переходу на отечественное ПО включают не только замену иностранного софта, но и обеспечение совместимости, безопасности и непрерывности бизнес-процессов.

3

Рост потребности в сертификатах

Рост использования приложений, применяющих сертификаты, а также повышение требований к защищённости коммуникаций, приводит к возрастающей потребности в цифровых сертификатах, росту объемов и требований к скорости выпуска.

Динамика выпуска сертификатов

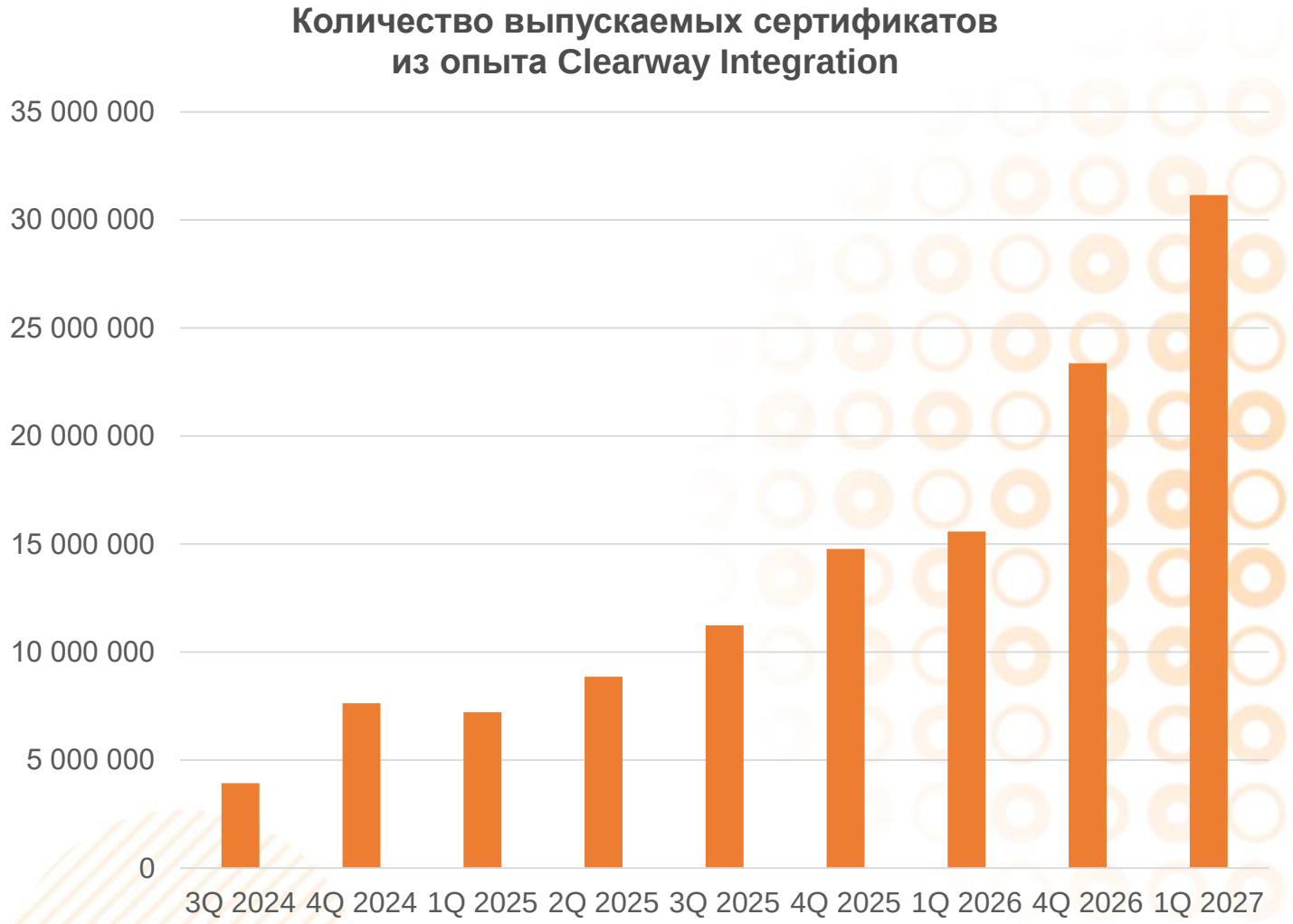
CLEARWAY INTEGRATION

Сокращение срока действия сертификатов

С 2027-го года — до 100, а к 2029 году — до 47 дней. При этом внедрение Zero Trust и mTLS делает сертификаты обязательными для каждого элемента инфраструктуры: пользователей, сервисов, API и микросервисов

Увеличение нагрузки на PKI

Тысячи сервисных соединений генерируют десятки тысяч запросов в минуту. Без автоматизации это неизбежно приводит к ошибкам и простоям критически важных сервисов



На примере кейса одной российской компании

Проблемы, которые решает Clearway CA

CLEARWAY INTEGRATION

1. Затраты на покупку сертификатов от коммерческих CA
2. Большие затраты на развертывание собственной PKI
3. Затраты на поддержку PKI
4. Высокие требования к квалификации персонала
5. Проблемы совместимости в разных ОС и приложениях
6. Проблемы импортозамещения PKI
7. Использование самоподписанных, wildcard и недоверенных сертификатов
8. Отсутствие квалифицированной поддержки вендора
9. Отсутствие единой совместимой экосистемы управления PKI

Преимущества использования Clearway CA

CLEARWAY INTEGRATION

1

Высокая скорость
Выпуск более 2000 сертификатов в минуту на одном сервере

2

Большие объемы
Выпуск миллионов сертификатов без просадки производительности

3

Безопасность
Ролевая модель, поддержка HSM, интеграция с системой хранения секретов

4

Удобный интерфейс
Графический интерфейс и утилита командной строки с широкими возможностями

5

Проверка статуса сертификатов
CRL и deltaCRL для актуальных списков отзыва, OCSP для мгновенной проверки в реальном времени

6

Сервис публикации
Копирование CRL и сертификатов на точки распространения и в объекты LDAP

7

Поддержка протоколов
Поддерживаются различные протоколы запроса сертификатов: SCEP, WSTEP, ACME, EST, CMP

8

Управление сертификатами
Автоматизация выпуска, отзыва и проверки статуса сертификатов

9

Поддержка алгоритмов
Возможен выпуск сертификатов с использованием алгоритмов RSA и ГОСТ, ECC/ECDSA

Цели продукта

CLEARWAY INTEGRATION

Импортозамещение

Продукт предназначен для выпуска технологических сертификатов.

Является альтернативой Microsoft CA.

Обеспечивает соответствие регуляторным требованиям и независимость от зарубежных решений.

Безопасность

Продукт обеспечивает выпуск сертификатов, используемых для защиты коммуникаций и других компонентов ИТ-инфраструктуры

Продукт имеет продвинутую ролевую модель, обеспечивает поддержку HSM, поддерживает журналирование в соответствии с требованиями регуляторов.

Сокращение ТСО

Высокая надёжность и автоматизация процессов уменьшают издержки на обеспечение безопасности и ликвидацию последствий инцидентов ИБ за счёт снижения доли ручных операций (в сравнении с использованием openssl), сокращения ошибок и ускорения реагирования.

Удобство

Продукт обеспечивает автоматизацию процессов, применение шаблонов и централизованного управления, что снижает нагрузку на администраторов и упрощает эксплуатацию PKI.

Как устроен Clearway CA

CLEARWAY INTEGRATION

WEB

Модульное web-приложение

Модули – web сервисы с интерфейсом API. К модулю Clearway CA можно подключать дополнительные – графический интерфейс, публикация CRL, OCSP, архивирование истекших сертификатов, модули поддержки протоколов запроса сертификатов;

SQL

Postgre SQL в качестве БД

Современная база данных обеспечивает быстродействие и хранение больших объемов сертификатов, позволяет использовать кластерную конфигурацию;

CSP

OpenSSL и КриптоПро CSP в качестве криптопровайдера

По умолчанию используется OpenSSL, входящий в большинство дистрибутивов Linux, в том числе российских сертифицированных. В качестве альтернативы может быть использован КриптоПро CSP;

HSM

Поддержка HSM

Обеспечивается хранение ключей ЦС с помощью специализированных аппаратных модулей посредством интерфейса PKCS11;

ЦС

Полноценная кластеризация

Поддерживается работа в виде массива серверов с единой базой данных и единым сертификатом ЦС. Все узлы кластера являются активными.

Clearway CA

CLEARWAY INTEGRATION

Наиболее важной функцией Центра Сертификации является

Выпуск и отзыв сертификатов

Выпуск сертификатов

Поддерживает выпуск сертификатов на основе CSR через веб-интерфейс, API и командную строку, а также по различным протоколам – SCEP, WSTEP, EST, ACME, CMP при помощи специальных модулей в составе ЦС.

Отзыв сертификатов

Поддерживает отзыв сертификатов через веб-интерфейс, API и командную строку, с указанием причины отзыва. Обеспечивает публикацию CRL и работу OCSP в реальном времени.

Автоматизация операций

Поддерживает возможность пакетного выпуска и отзыва сертификатов, синхронизацию шаблонов с другими ЦС, автоматическое архивирование истекших сертификатов и т.д.

Clearway CA

CLEARWAY INTEGRATION

Наряду с выпуском и отзывом сертификатов ЦС выполняет другую важную функцию -

Предоставление информации о выпущенных сертификатах

Публикация CRL

Поддерживает публикацию CRL и Delta CRL в точки распространения, обеспечивает их регулярное обновление и доступность для проверки статуса сертификатов;

Поддержка протокола OCSP

Поддерживает протокол OCSP, обеспечивающий онлайн проверку статуса сертификатов в режиме, близком к реальному времени, с получением актуального состояния без необходимости загрузки CRL;

Веб-интерфейс

Веб-интерфейс обеспечивает оперативное получение информации о сертификатах, включая статус, атрибуты и параметры, с поддержкой поиска, фильтрации и просмотра карточек сертификатов;

Формирование отчетов

Поддержка формирования отчетов по сертификатам, шаблонам, запросам и событиям с помощью веб-интерфейса с применением поиска, фильтров, настройкой выборки и экспортом результатов в файл.

Сравнение с Microsoft CA

CLEARWAY INTEGRATION

	Microsoft CA	Clearway CA
Архитектура	Часть Windows	Модульная
Серверная ОС	Windows	Linux
База данных	ESE, файловая	Postgre SQL
Служба каталогов	Active Directory	Active Directory, ALD Pro, РЕД АДМ, Samba, FreeIPA и т.п.
Графический интерфейс	MMC, Web Enrollment	Web-интерфейс с широкими возможностями управления сертификатами
Интерфейсы	DCOM, SOAP	REST API
Дополнительные компоненты	CEP\CES, Web Enrollment, OCSP, NDES	Графический интерфейс, OCSP, Сервис публикации, Сервис архивирования истекших сертификатов
Поддержка протоколов	WCCE(DCOM), WSTEP, SCEP	SCEP, WSTEP, EST, ACME, CMP
Права доступа	Требуется Enterprise Admins	Гибкая ролевая модель, не требующая прав администратора СК
Автоматизация выпуска сертификатов	Autoenrollment только для доменных Windows клиентов	Автоматический выпуск на любой ОС с помощью агента
Отказоустойчивость	Кластеризация Generic Service, с одним активным узлом	Web-ферма с кластером Postgre SQL, все узлы активны
Хранение конфигурации	Параметры реестра без пояснений, множество отсутствующих по умолчанию значений	Все параметры присутствуют по умолчанию и имеют пояснения
Наличие систем управления PKI и сертификатами	Облачные решения Microsoft Cloud PKI и Microsoft Intune Certificate Connector	ЕСАУС – Единая Система Автоматического Управления Сертификатами СМИОК – Система Мониторинга Инфраструктуры Открытых Ключей ЛКПС – Личный Кабинет Пользователя Сертификатов

Архитектура Clearway CA

CLEARWAY INTEGRATION

Пользовательский доступ и клиентские интерфейсы

На слайде представлен набор серверных компонентов, обеспечивающих доступ пользователей, административное управление, аутентификацию и работу с сертификатами:

Прокси обеспечивает прием и маршрутизацию клиентских запросов к внутренним сервисам.

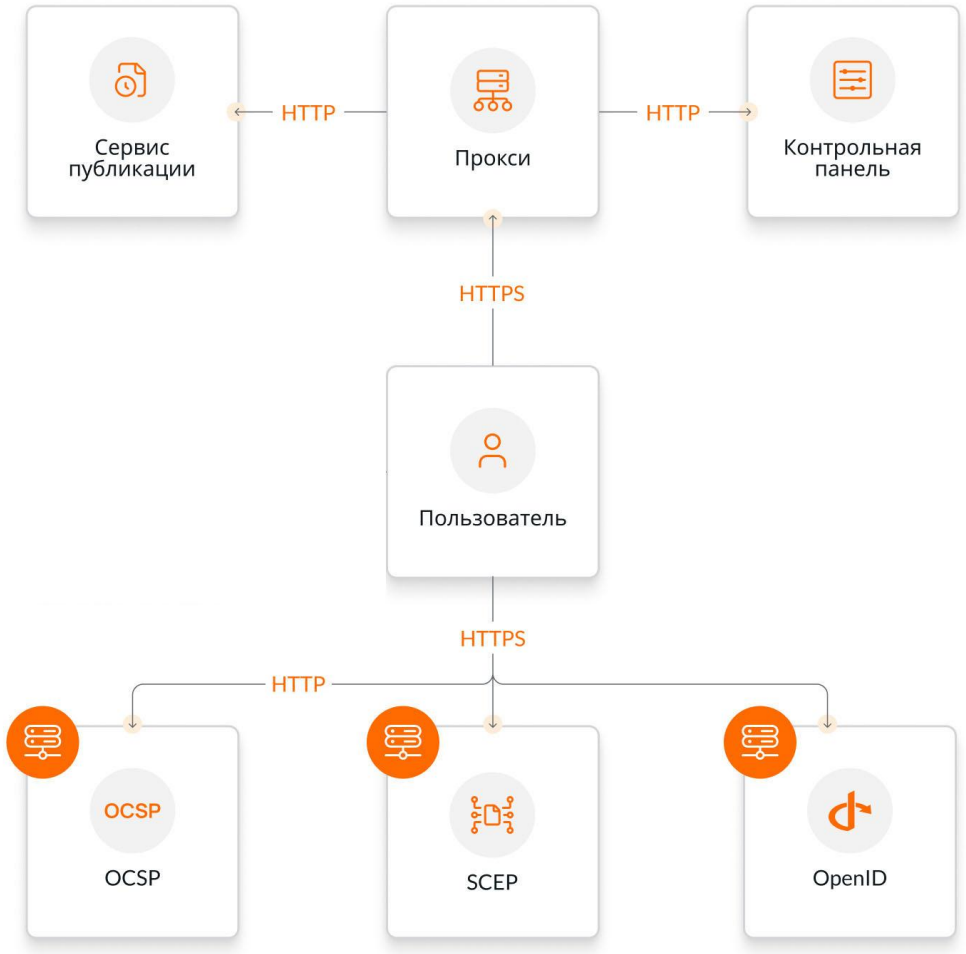
Контрольная панель обеспечивает выполнение административных операций через пользовательский интерфейс.

OpenID отвечает за авторизацию пользователей, а также за выдачу и отзыв JWT.

SCEP отвечает за обработку запросов на выпуск и обновление сертификатов по протоколу SCEP.

OCSP отвечает за предоставление информации о статусе сертификатов по протоколу OCSP.

Сервис публикации отвечает за публикацию файлов CRL по расписанию, а также за выполнение внеочередной публикации по API-запросу.



Архитектура Clearway CA

CLEARWAY INTEGRATION

Внутренние взаимодействия сервисов PKI

На слайде представлены внутренние взаимодействия сервисов PKI, обеспечивающих выполнение основных функций системы:

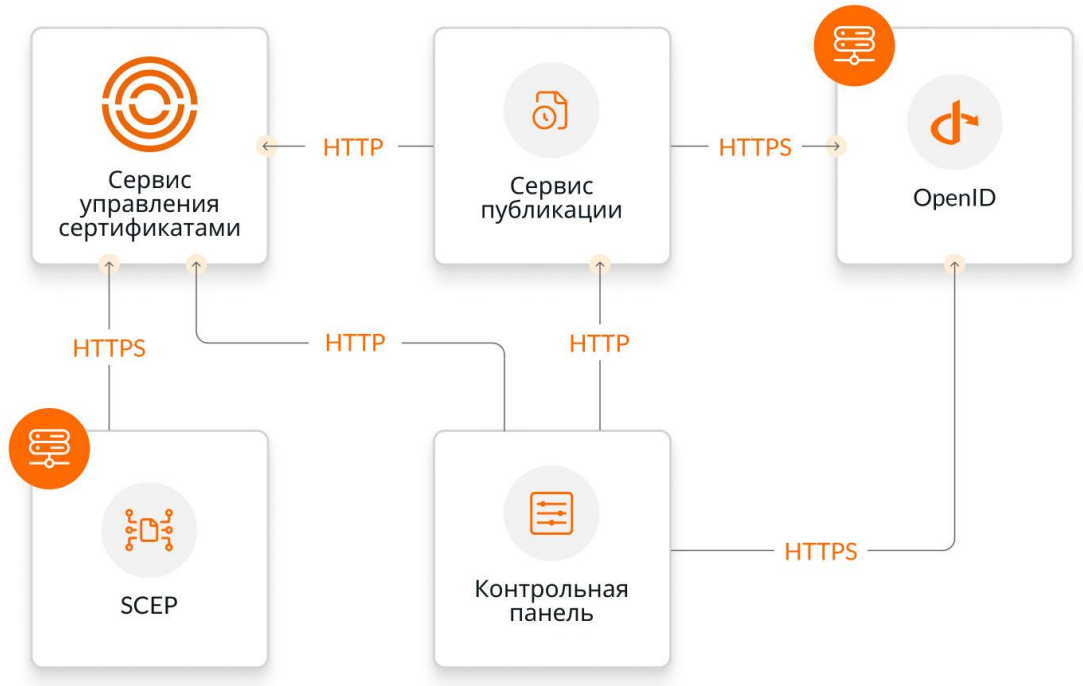
Контрольная панель принимает запросы пользователей и взаимодействует с OpenID, сервисом управления сертификатами и сервисом публикации.

Сервис управления сертификатами выполняет основные операции центра сертификации, включая выпуск и отзыв сертификатов.

SCEP (а также другие модули поддержки протоколов запроса сертификатов) принимает запросы на выпуск и обновление сертификатов и передает их в сервис управления сертификатами.

OpenID отвечает за аутентификацию пользователей, выпуск и отзыв JWT-токенов.

Сервис публикации получает данные сертификатов от сервиса управления сертификатами и выполняет публикацию CRL.



Архитектура Clearway CA

CLEARWAY INTEGRATION

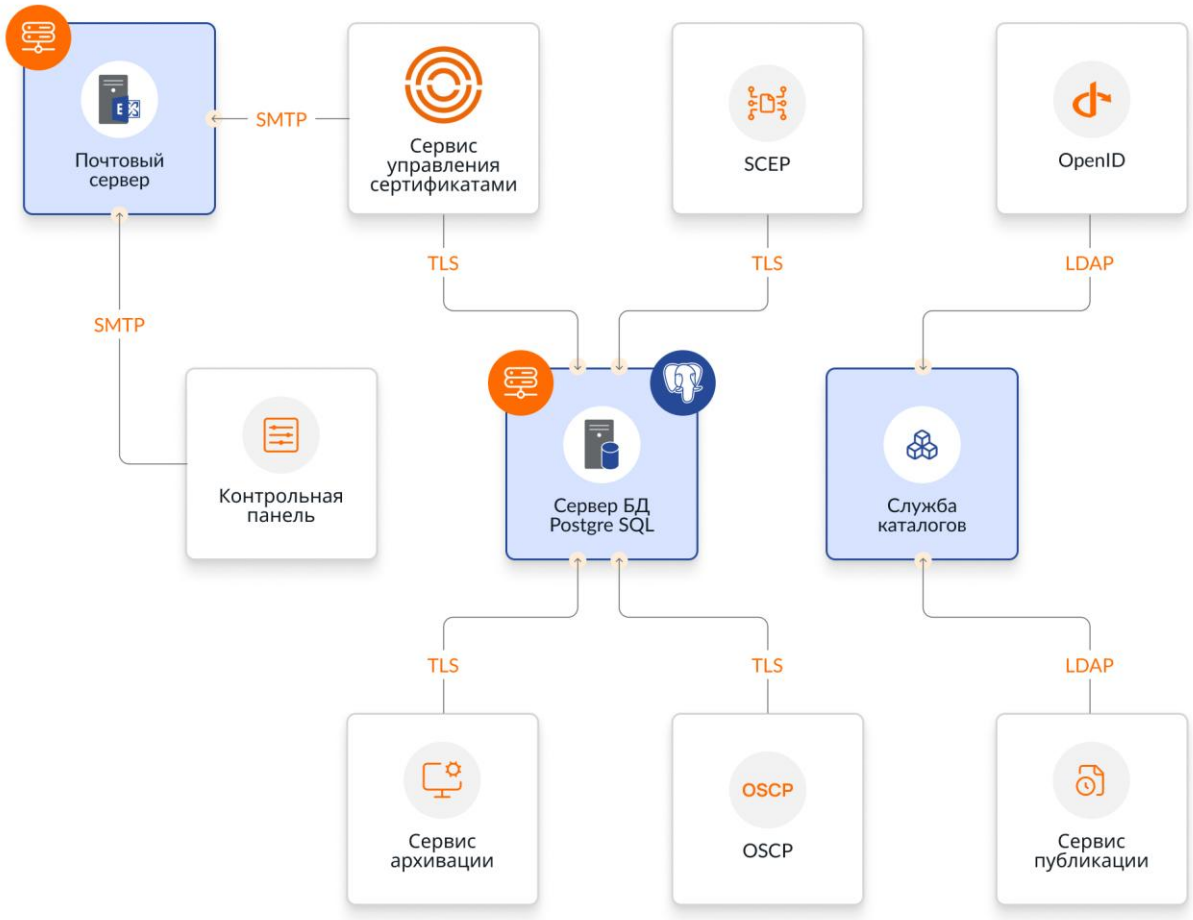
Взаимодействие с инфраструктурными сервисами

На слайде представлено взаимодействие компонентов системы с инфраструктурными сервисами:

Почтовый сервер используется для отправки служебных сообщений и уведомлений по протоколу SMTP.

Сервер БД PostgreSQL используется для централизованного хранения и предоставления данных, необходимых для работы серверных компонентов системы, включая выполнение операций с сертификатами и проверку их статуса.

Служба каталогов используется для хранения и предоставления данных, необходимых для авторизации пользователей и публикации сертификатов в объекты каталога.



Сценарии использования Clearway CA

Корневой ЦС

- Предназначен для формирования доверенной корневой точки и обеспечения криптографической целостности инфраструктуры PKI;
- Выступает в качестве точки доверия в рамках домена организации;
- Осуществляет подписание сертификатов подчинённых (выдающих) удостоверяющих центров;
- Большую часть времени выключен.

Выдающий ЦС

- Осуществляет выпуск и подписание сертификатов конечных субъектов (пользователей, сервисов, устройств);
- Может функционировать как универсальный (многоцелевой) или специализированный (для отдельных типов сертификатов/сценариев применения);
- Поддерживает режимы выпуска: автоматический и с предварительным подтверждением.

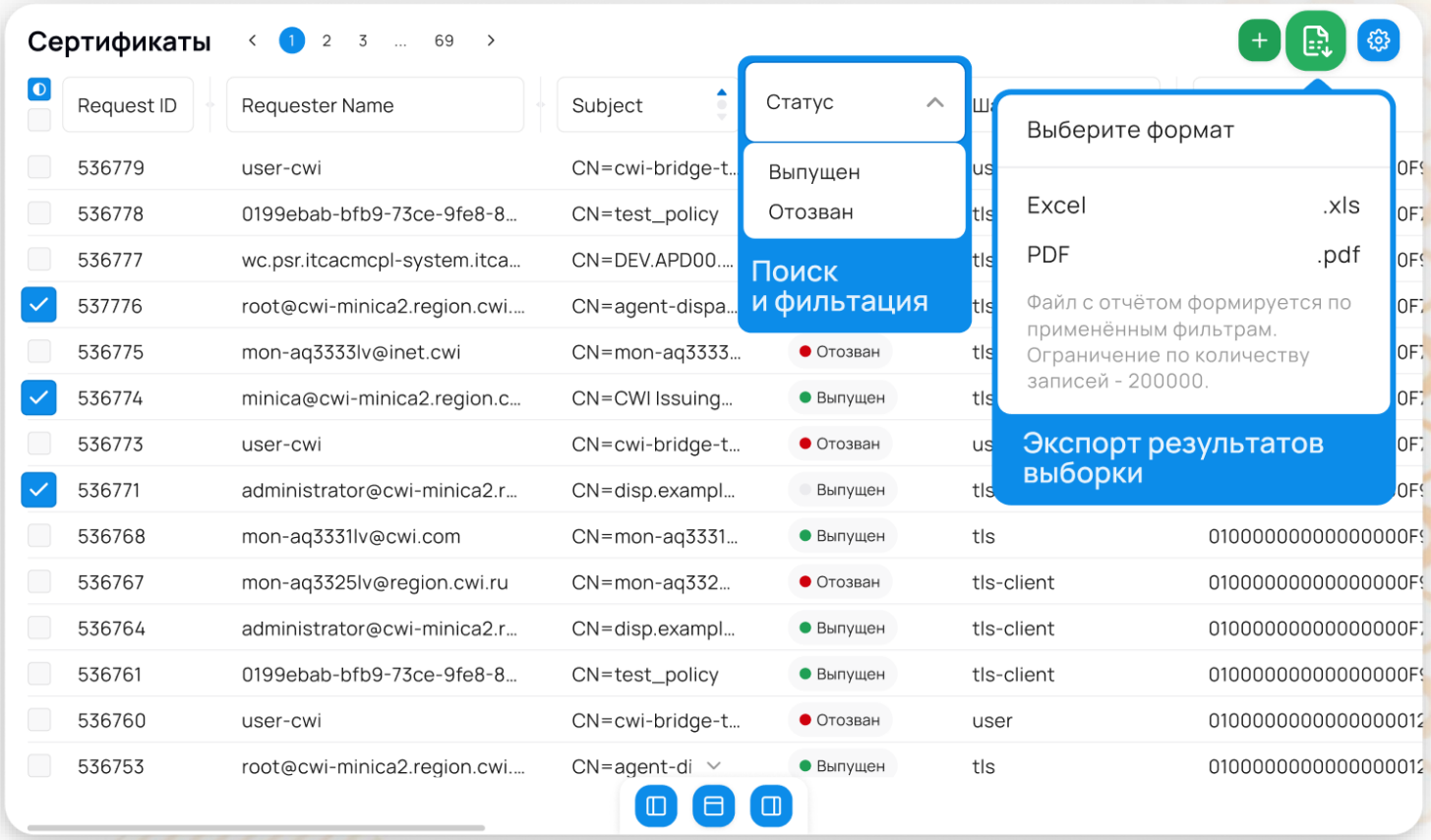
Список сертификатов

Список сертификатов представляет собой совокупность записей о сертификатах, выпущенных ЦС, за исключением сертификатов, сформированных по шаблонам с признаком запрета сохранения в базе данных (nodb).

Список обеспечивает расширенный поиск и фильтрацию сертификатов по ключевым атрибутам.

Поддерживается выполнение операций над несколькими сертификатами (пакетная обработка).

Поддерживается экспорт результатов выборки в файл.



Шаблоны сертификатов

CLEARWAY INTEGRATION

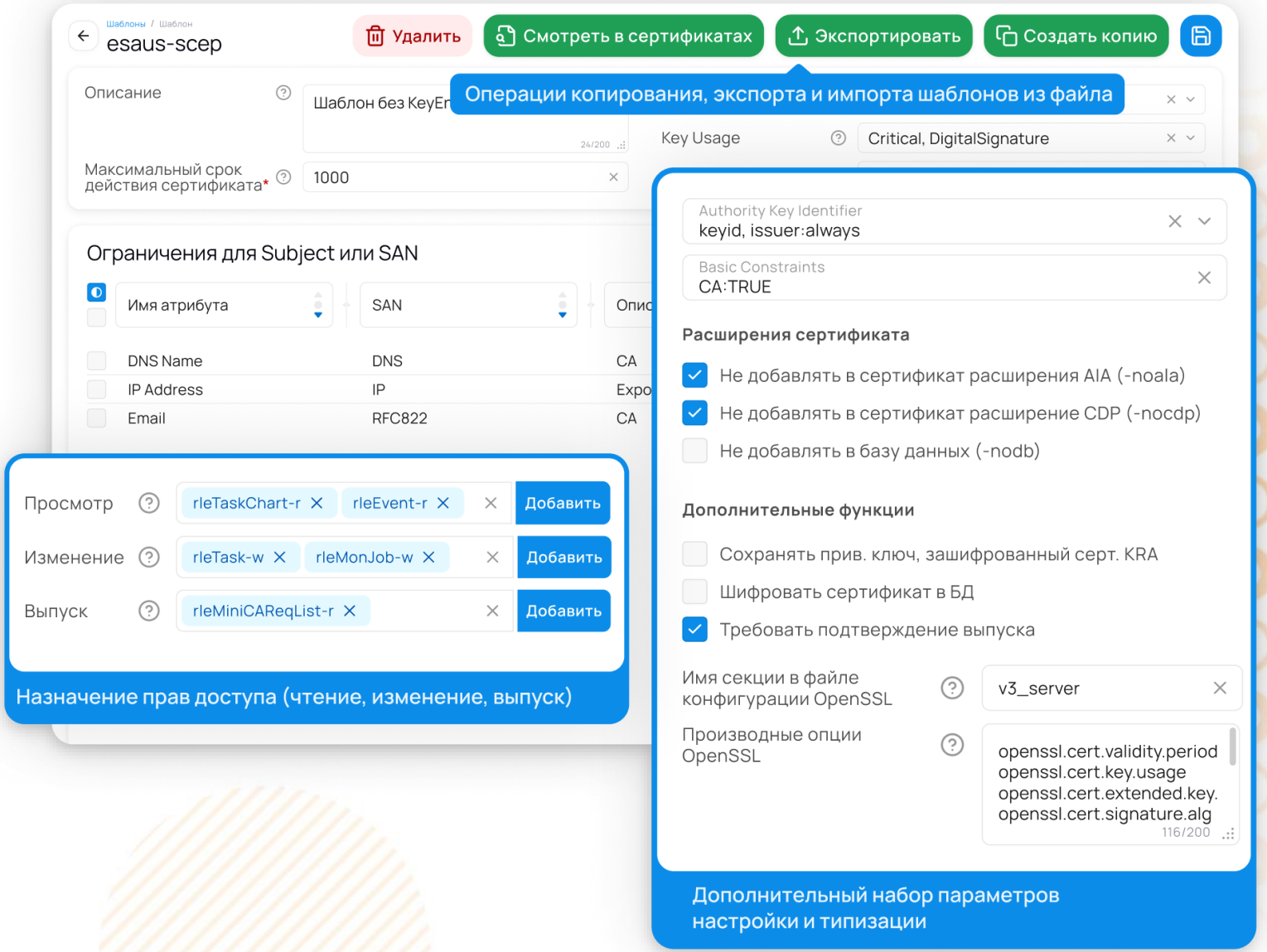
Шаблоны определяют структуру запроса и состав сертификата, обеспечивая контроль атрибутов и ограничений.

Шаблоны включают ограниченный набор ключевых параметров, подлежащих настройке и типизации.

Обеспечивается контроль состава и структуры атрибутов Subject и SAN.

Поддерживаются операции копирования, экспорта в файл и импорта шаблонов из файла.

Поддерживается назначение прав доступа (чтение, изменение, выпуск) на уровне отдельных шаблонов.



Проверка имен в шаблонах

CLEARWAY INTEGRATION

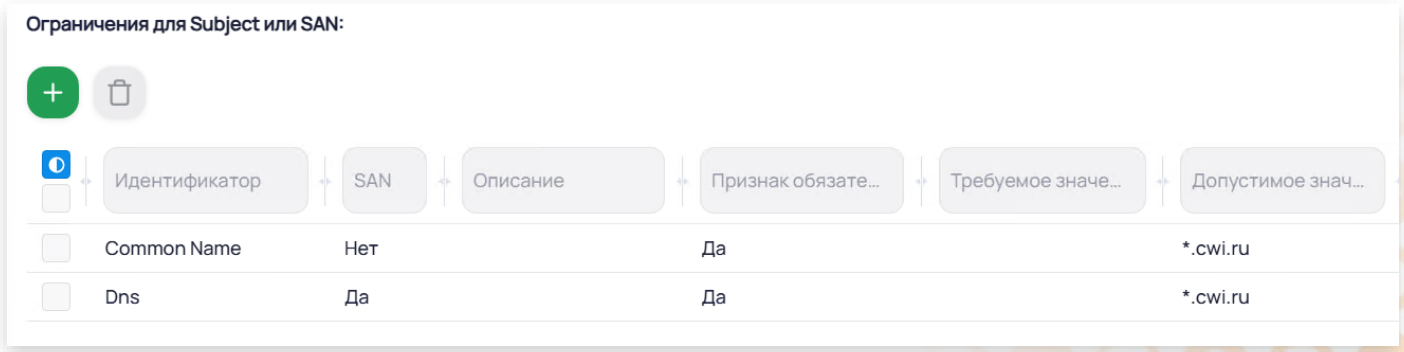
Шаблоны сертификатов позволяют гибко контролировать содержание атрибутов Subject и SAN;

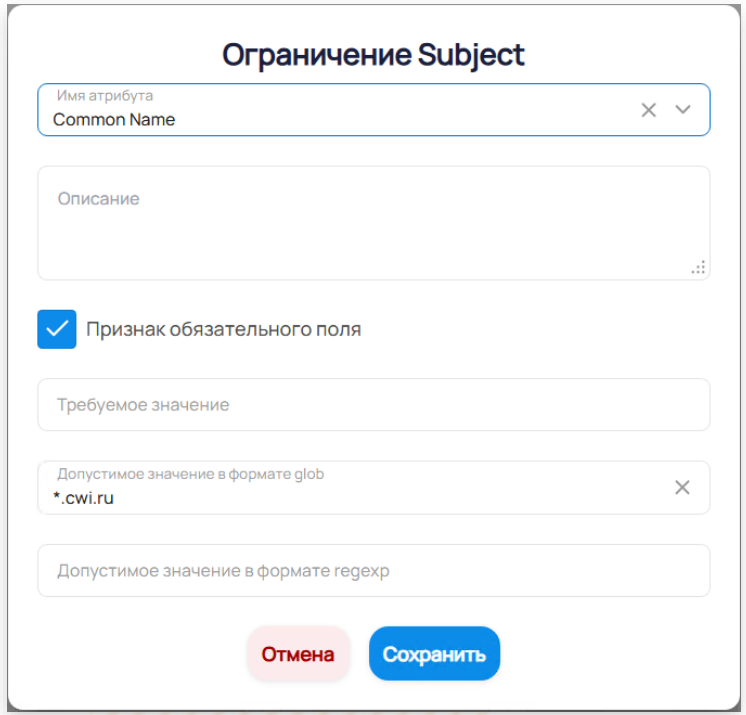
Можно задать ограничение на любой RDN в Subject и любой тип SAN;

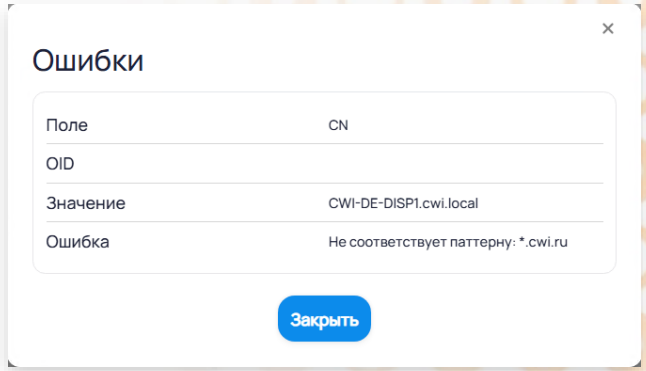
Ограничений может быть несколько, все они должны выполняться;

Можно сделать поле обязательным с любым значением, либо прямо задать требуемое значение;

Можно задать шаблон имени в виде регулярного выражения.







Выпуск сертификата с помощью CSR

CLEARWAY INTEGRATION

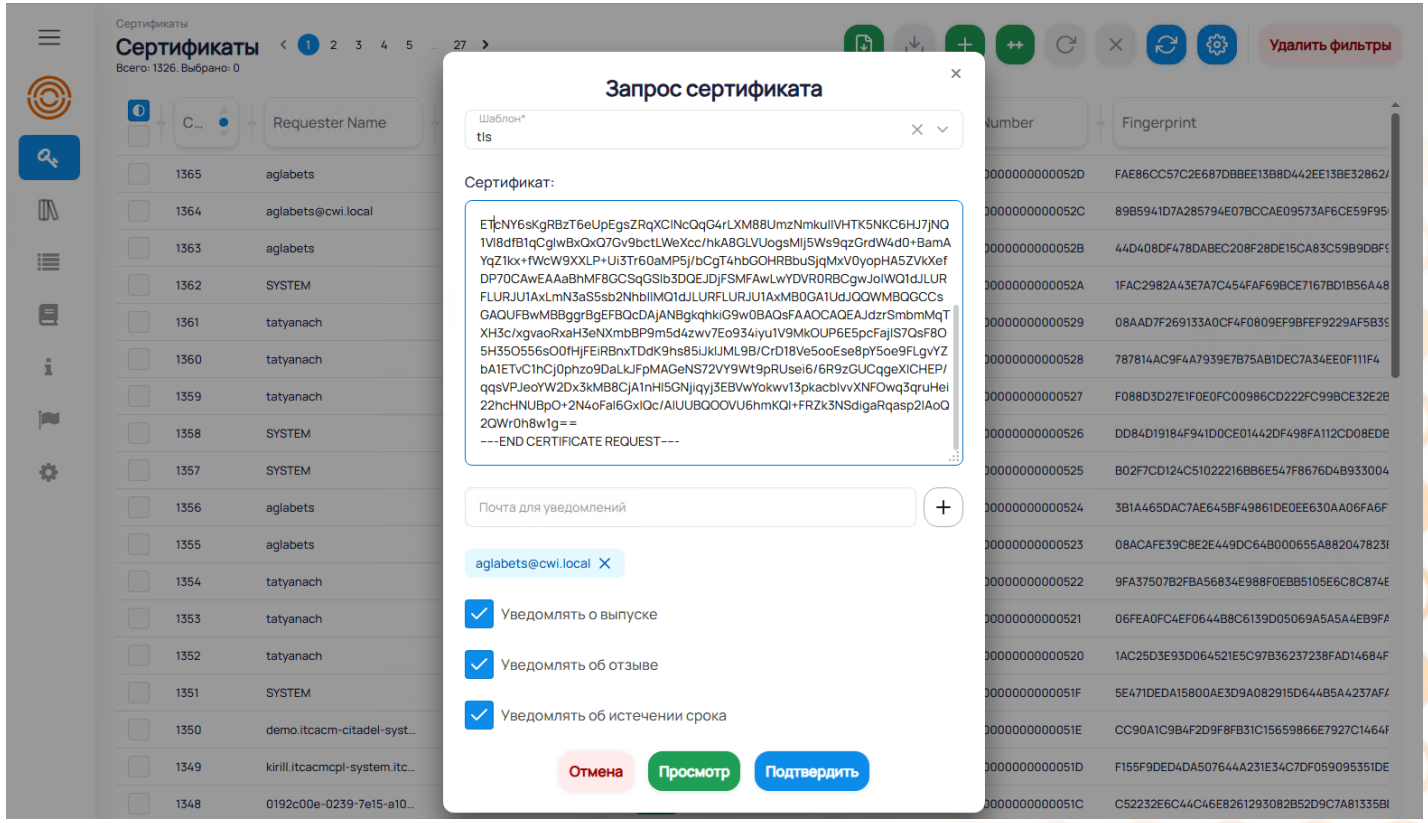
При выпуске используются шаблоны для автозаполнения атрибутов и контроля их содержания;

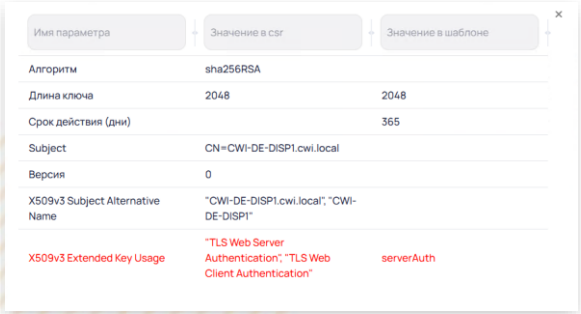
Указать CSR можно в виде файла или текста;

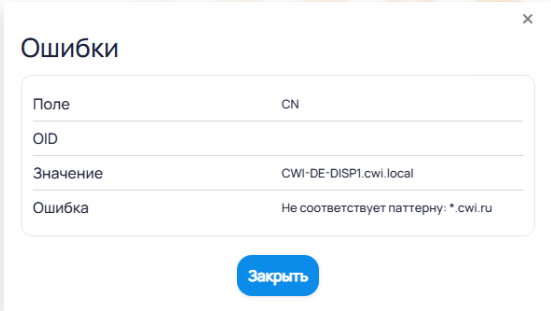
Предварительный просмотр CSR и сравнение с шаблоном. Подсветка несоответствующих атрибутов;

Возможно указание e-mail для оповещения по основным событиям жизненного цикла;

При расхождении с шаблоном неизменяемых атрибутов будет отказ в выдаче. Изменяемые атрибуты переопределяются в соответствии с шаблоном.







Выпуск сертификата через модули протоколов

CLEARWAY INTEGRATION

В состав Clearway CA входит ряд модулей поддержки протоколов запроса сертификатов - SCEP, WSTEP, EST, ACME, CMP;

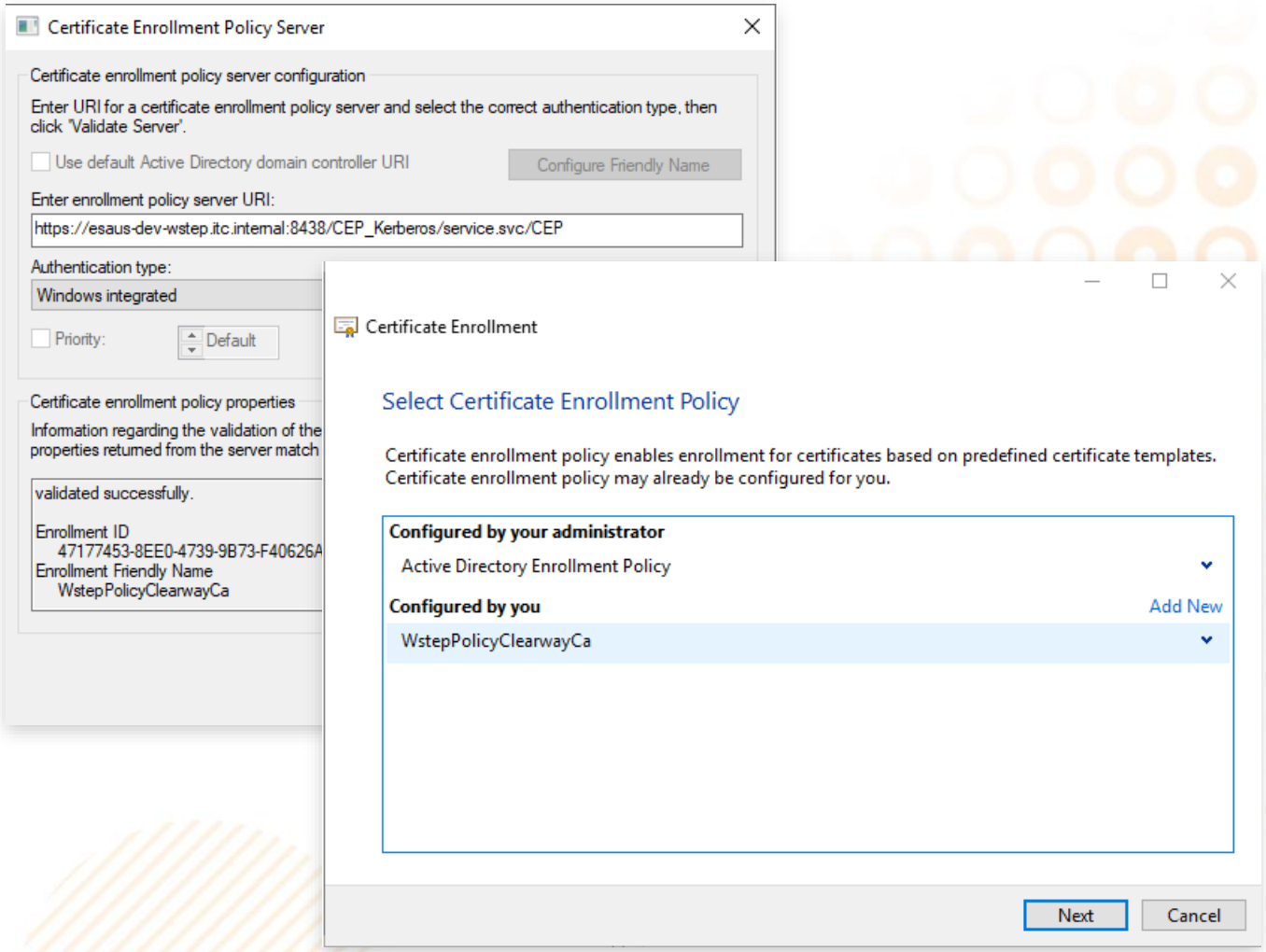
Модули протоколов позволяют обеспечить выпуск сертификатов для различных клиентов привычным для них способом;

Модуль протокола WSTEP позволяет выпускать сертификаты на Windows встроенными инструментами, в том числе с помощью Autoenrollment;

Модуль поддержки SCEP обеспечивает поддержку сетевых и мобильных устройств;

Модуль ACME обеспечивает поддержку приложений Certbot, Nginx, Apache HTTP Server и т.д.

Модуль EST обеспечивает поддержку сетевого оборудования, устройств IoTи т.д.



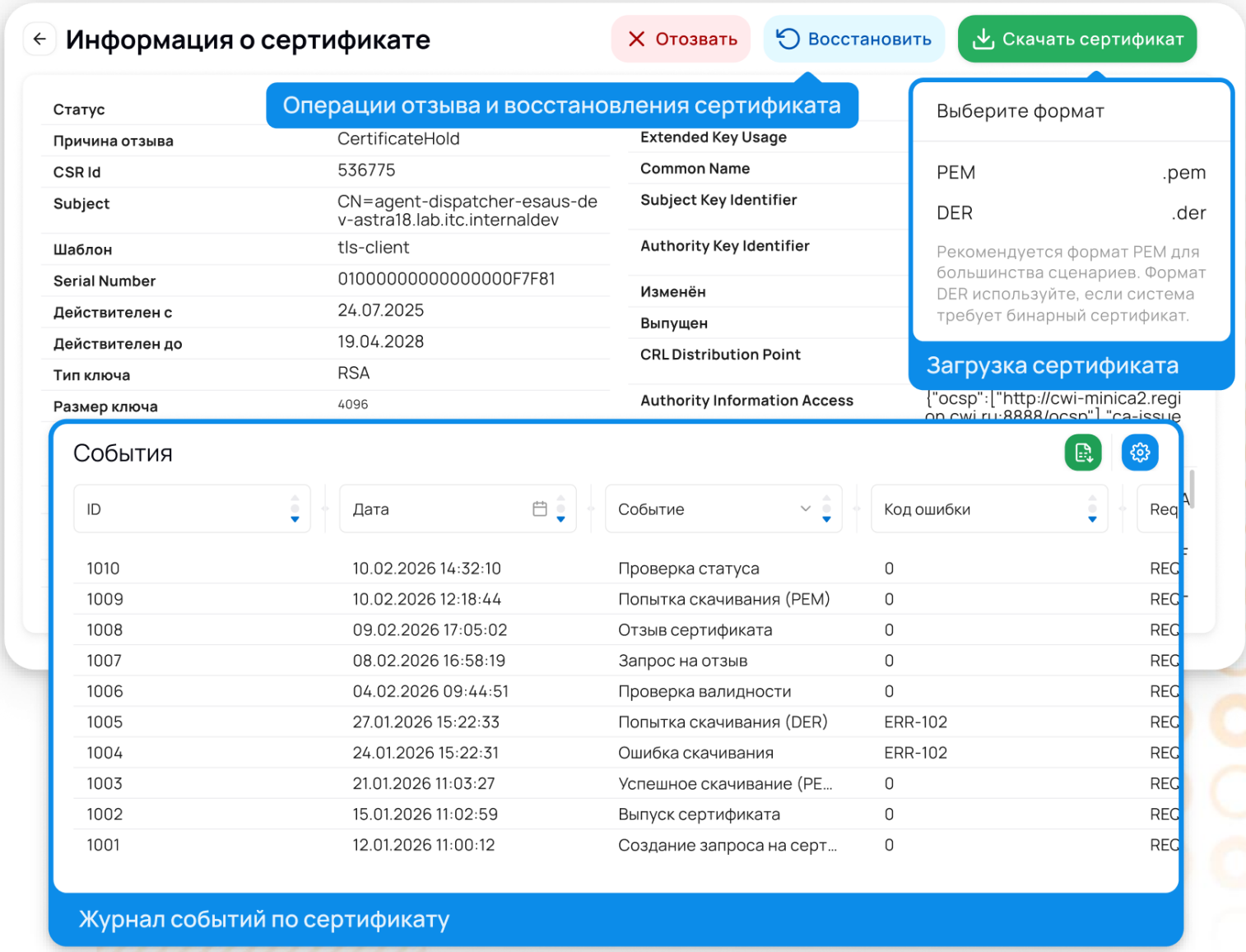
Карточки сертификатов

Карточка сертификата содержит полный набор атрибутов (Subject, SAN, EKU, параметры ключа, срок действия и др.);

Отображается полный журнал событий по сертификату с момента его создания, включая операции выпуска, изменения статуса, отзыва и иные действия;

В карточке предусмотрена возможность скачивания сертификата в формате PEM или DER;

Поддерживаются операции отзыва сертификата и восстановления ранее отозванного сертификата.



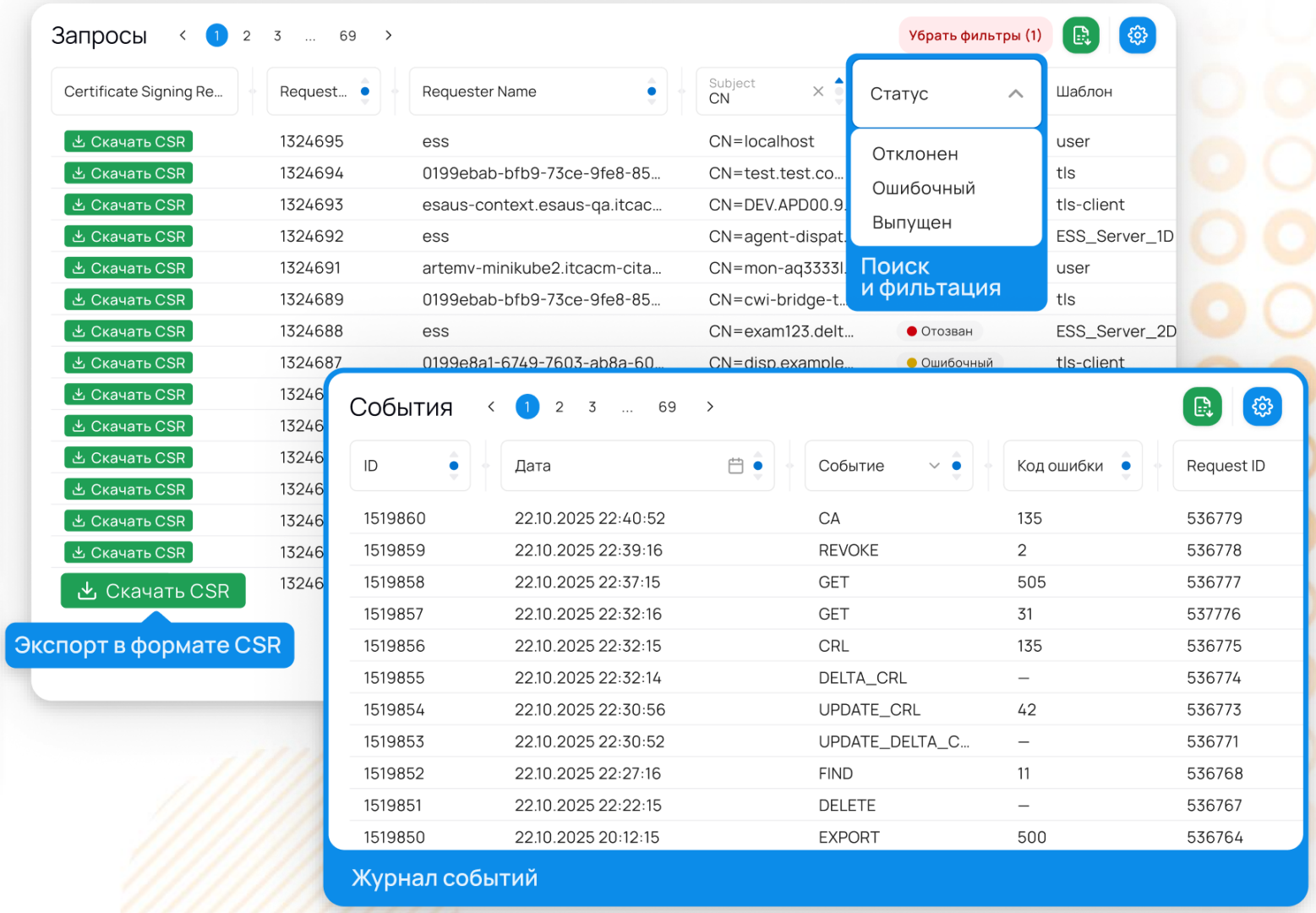
Журналы и запросы событий

CLEARWAY INTEGRATION

В базе данных центра сертификации ведутся два журнала: журнал запросов и журнал событий.

Журнал запросов содержит все поступившие в ЦС запросы на выпуск сертификатов, с возможностью поиска, фильтрации и экспорта в формате CSR.

Журнал событий содержит записи обо всех операциях в ЦС (выпуск, отзыв, публикация CRL и др.).



Информация о CRL

Предусмотрена специализированная страница для получения информации об актуальных версиях CRL и Delta CRL.

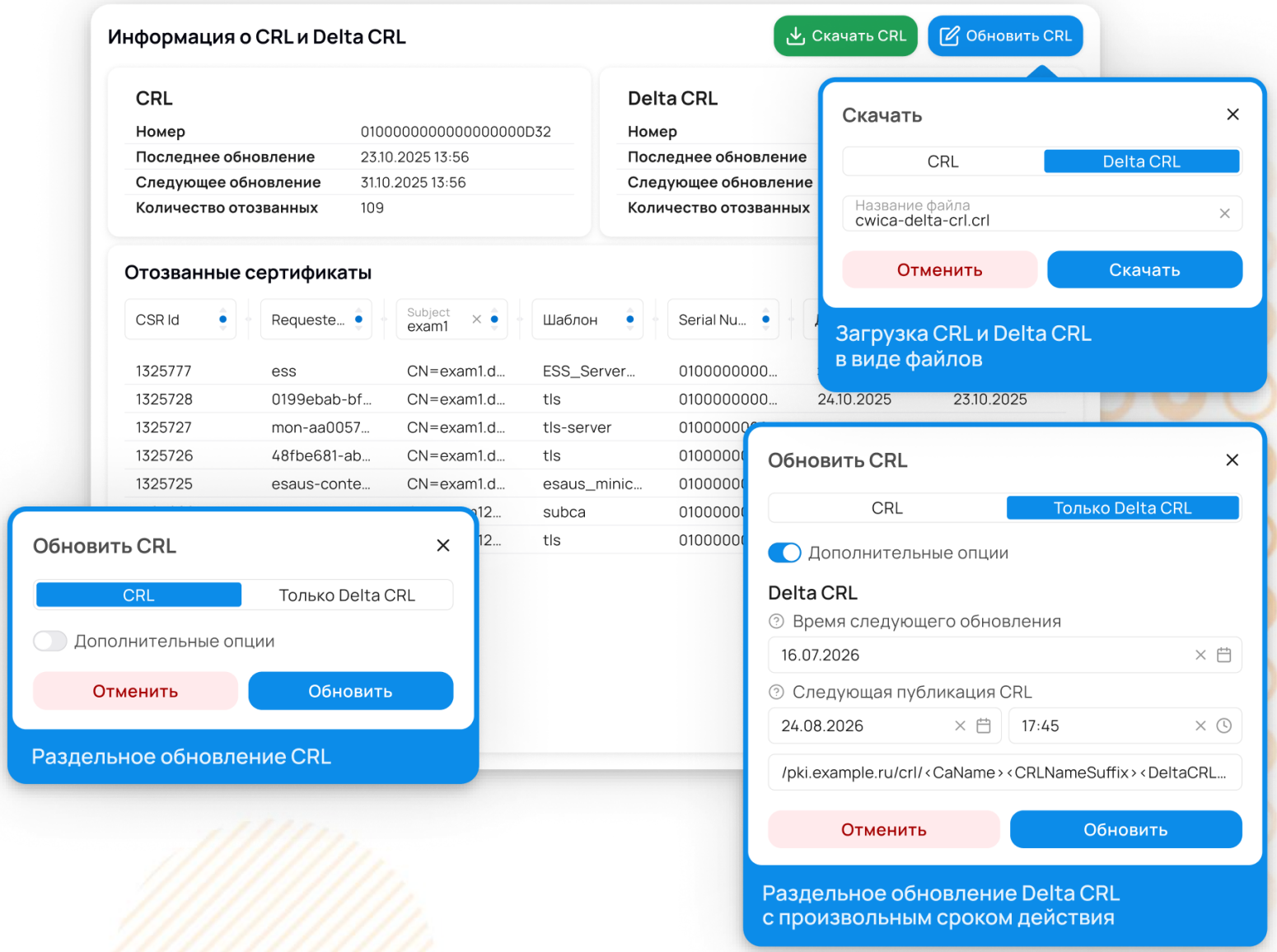
На странице также отображается перечень всех отозванных сертификатов.

Список отозванных сертификатов содержит сведения о текущем CRL, в котором они опубликованы.

Предусмотрена возможность загрузки CRL и Delta CRL в виде файлов.

Раздельное обновление CRL и Delta CRL позволяет оперативно публиковать изменения статусов сертификатов.

При обновлении CRL может быть задан произвольный срок его действия.



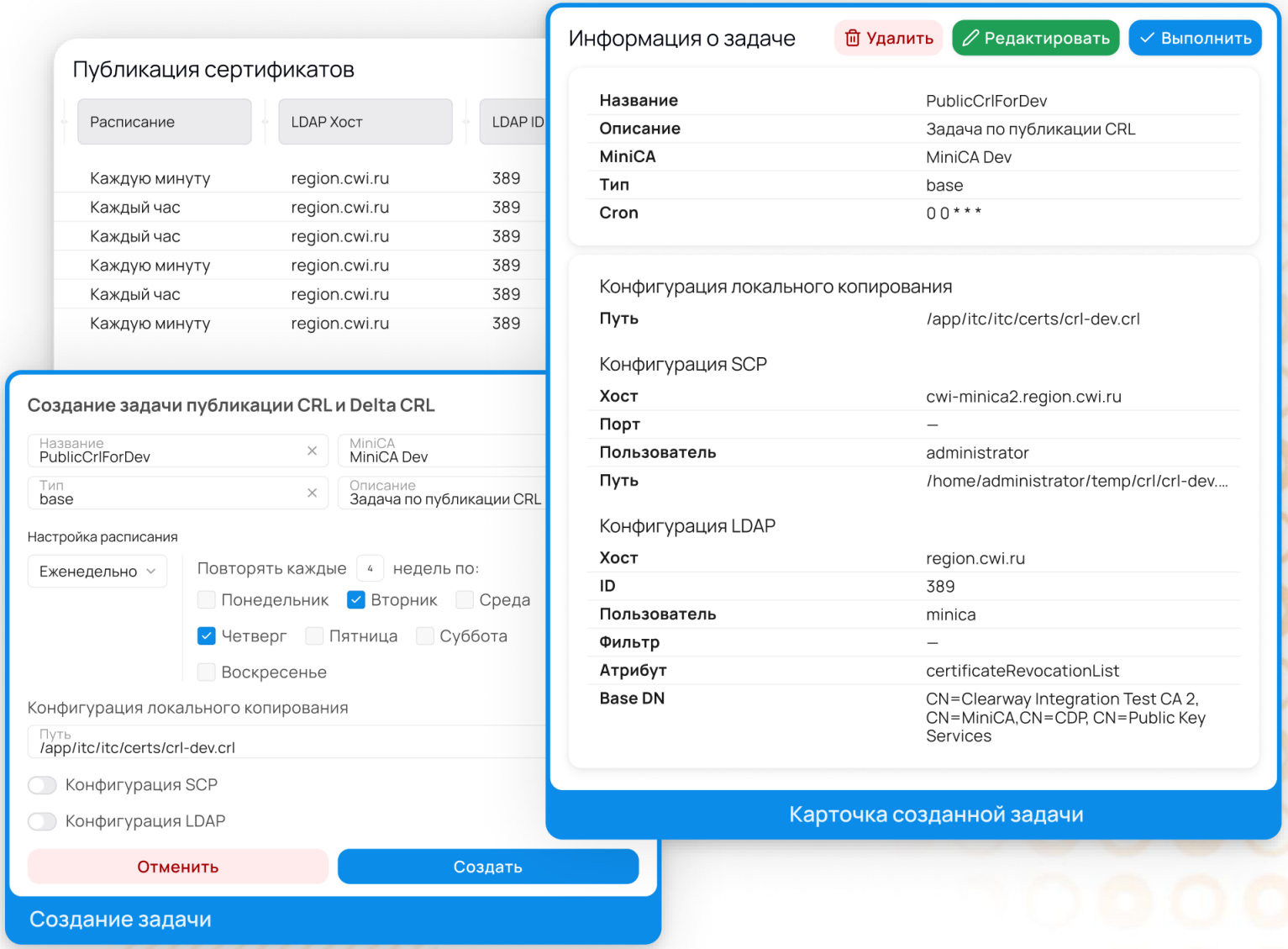
Сервис публикации

Обеспечивает публикацию CRL и сертификатов посредством копирования в файловые ресурсы (SCP, SMB) и записи в LDAP-каталог.

Выделенный сервис публикации повышает безопасность ЦС и обеспечивает гибкость сценариев распространения CRL и сертификатов.

В рамках задачи поддерживается публикация CRL на несколько целевых ресурсов.

Создание задач осуществляется через графический интерфейс.



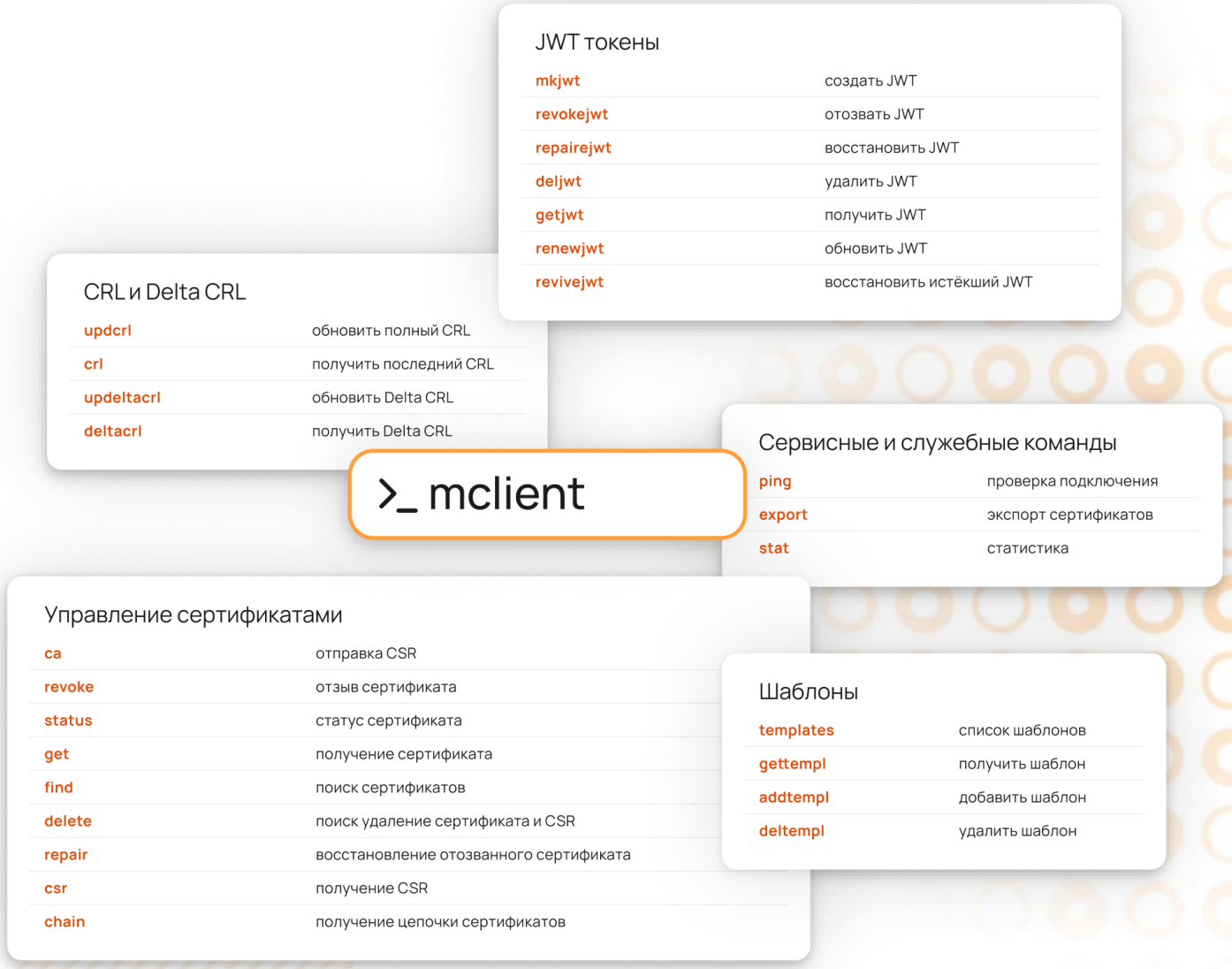
Инструмент командной строки

CLEARWAY INTEGRATION

Клиентская утилита mclient обеспечивает выполнение всех операций управления ЦС из командной строки.

Инструмент командной строки обеспечивает автоматизацию операций и поддержку сценариев пакетного выпуска сертификатов.

Позволяет управлять ЦС без установки Контрольной панели, что удобно для эксплуатации корневого ЦС и специализированных сценариев работы с выдающими ЦС.

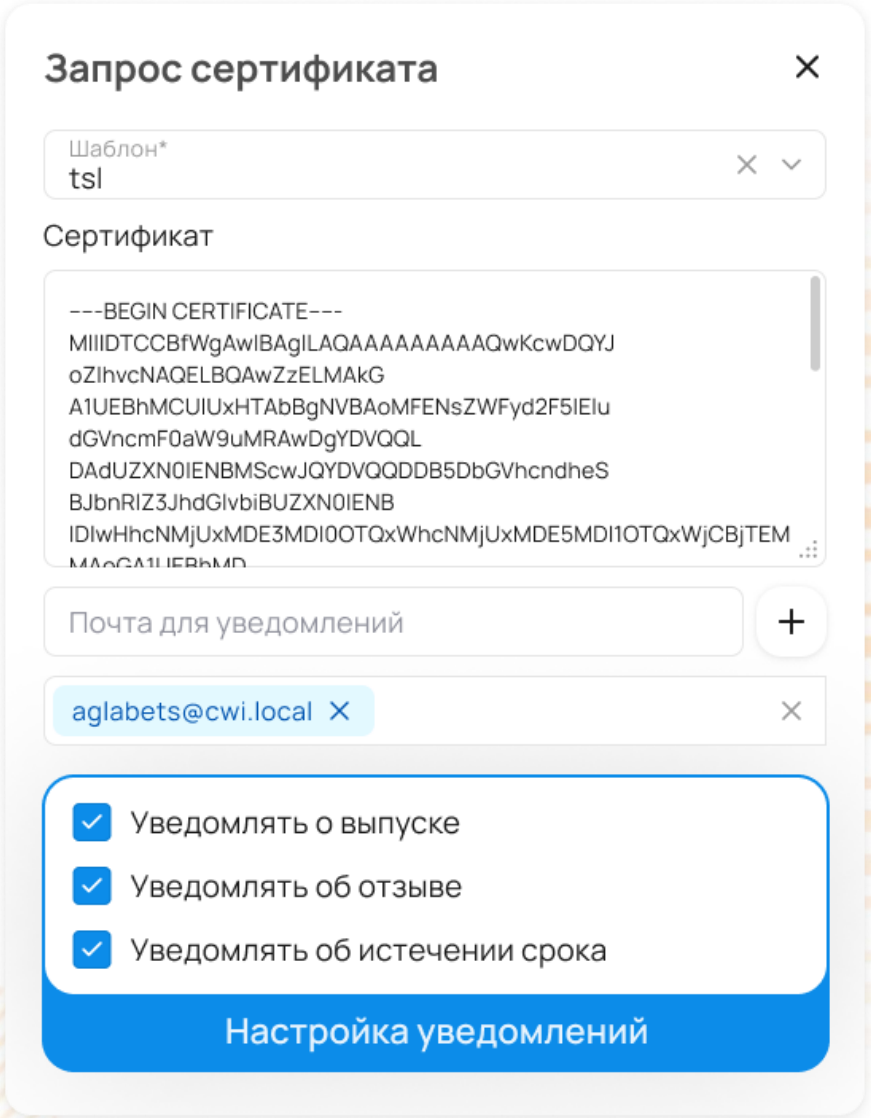


Отправка почтовых уведомлений

CLEARWAY INTEGRATION

Контрольная панель Clearway CA поддерживает механизм уведомлений по событиям жизненного цикла сертификатов:

- выпуск сертификата;
- отзыв сертификата;
- приближение срока истечения сертификата за заранее заданное количество дней;



API для интеграции

Clearway CA предоставляет полный API для синхронизации данных и управления, включая операции загрузки и выгрузки сертификатов и шаблонов, выгрузку журналов запросов и событий, а также выполнение управляющих команд.

Clearway CA поддерживает интеграцию с продуктами экосистемы ЦУГИ и внешними системами:

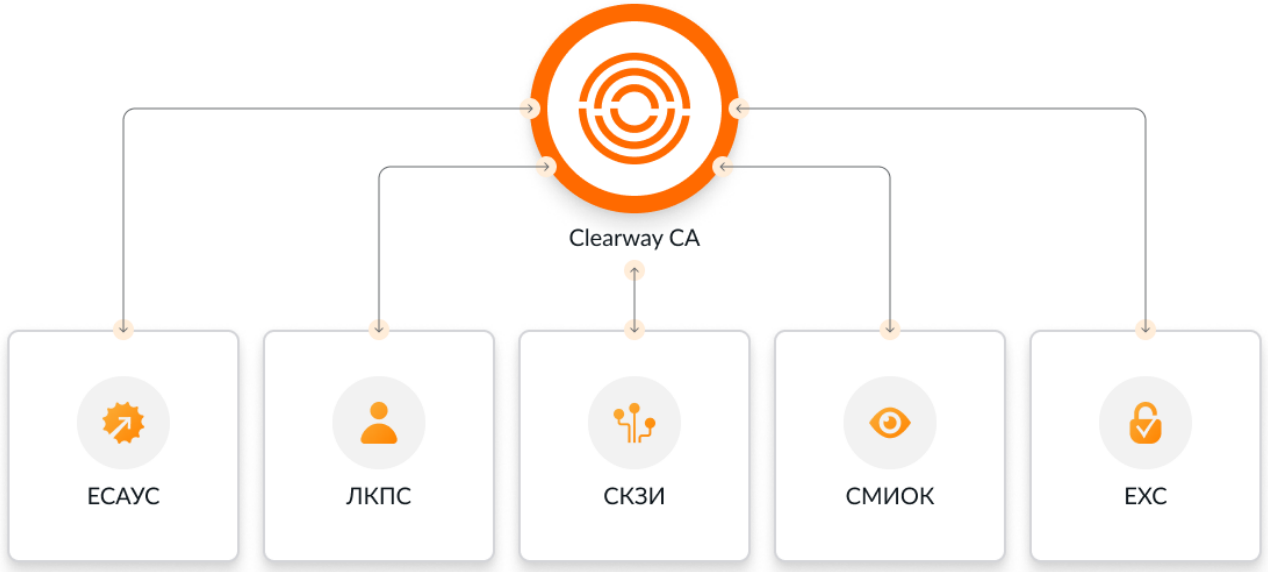
ЕСАУС – единая система Автоматического управления сертификатами;

ЛКПС – личный кабинет пользователя сертификатов;

СМИОК – система мониторинга инфраструктуры открытых ключей;

СУУ СКЗИ – система управления и учета СКЗИ;

ЕХС – единая система хранения секретов.



Интеграция с ЦУГИ ЕСАУС

ЕСАУС — Единая Система Автоматического Управления Сертификатами.

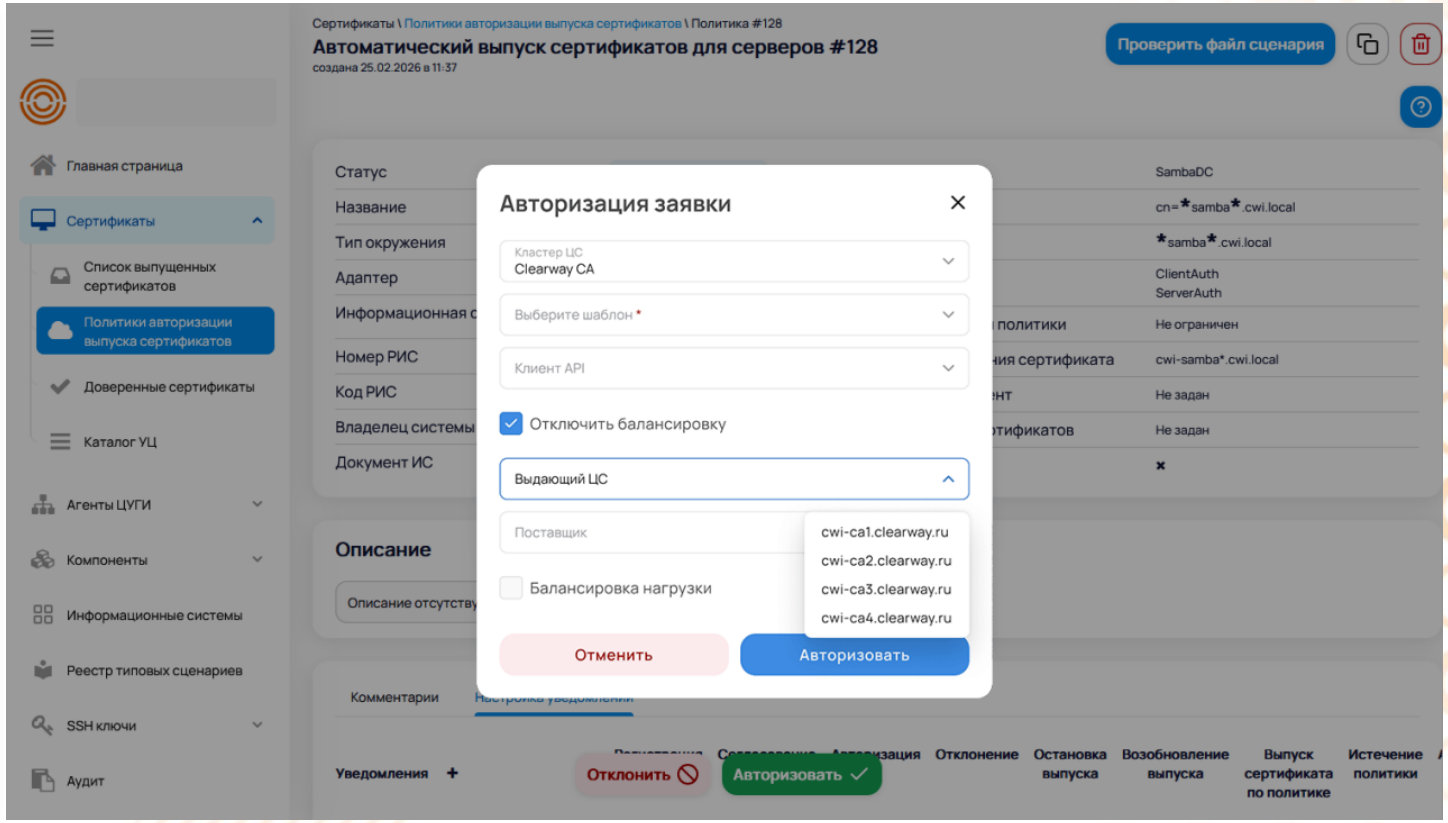
Цель интеграции – автоматический выпуск и обновление сертификатов на клиентах

Автоматический выпуск сертификатов — ЕСАУС использует Clearway CA для автоматизации выпуска, доставки и установки в том числе доверенных сертификатов самих ЦС;

Применение политик — ЕСАУС использует сложные политики выпуска в дополнение к шаблонам Clearway CA, что позволяет очень гибко настраивать выпуск сертификатов;

Отказоустойчивость — ЕСАУС работает с несколькими экземплярами Clearway CA и отключает от выпуска недоступные узлы;

Балансировка нагрузки — ЕСАУС распределяет нагрузку между несколькими экземплярами Clearway CA;



Интеграция с ЦУГИ ЛКПС

ЛКПС — личный кабинет пользователя сертификатов.

Цель интеграции – контроль жизненного цикла выпущенных сертификатов

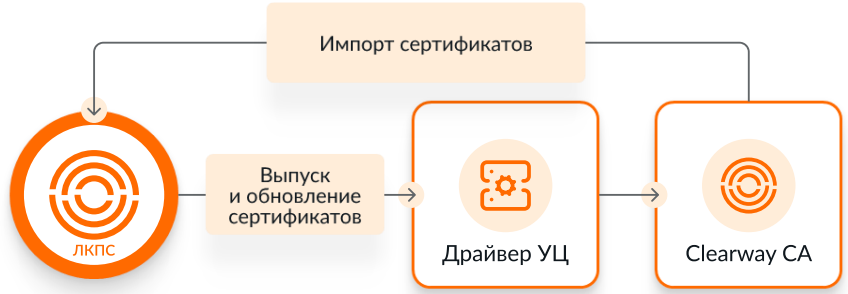
Хранение сертификатов — ЛКПС хранит все сертификаты организации и информацию о секретах, позволяя отслеживать их жизненный цикл;

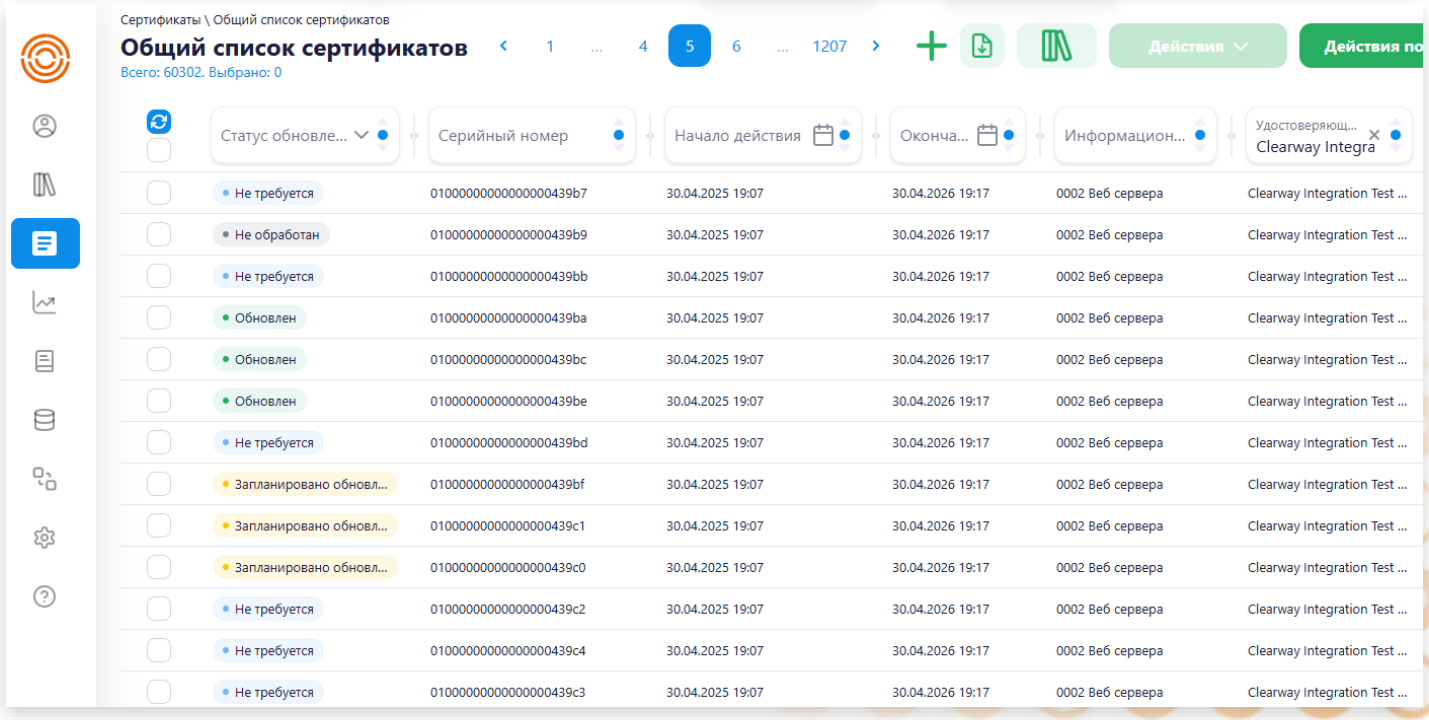
Автоматический поиск мест установки — система сама находит, где установлены сертификаты, за счёт интеграций со смежными продуктами ЦУГИ и другими системами организации;

Автоматическое назначение ответственных — ЛКПС сам назначает ответственных и отправляет почтовые уведомления с учётом кадрового статуса, опираясь на встроенный справочник контактов;

Справочник информационных систем — позволяет привязывать к сертификатам информационные системы и организационные единицы;

Самостоятельное указание статуса — пользователь может сам указать статус сертификата, назначить ответственных и привязать справочную информацию.





Интеграция с ЦУГИ СМИОК

СМИОК — система мониторинга ИОК.

Цель интеграции – мониторинг ЦС и смежных компонентов

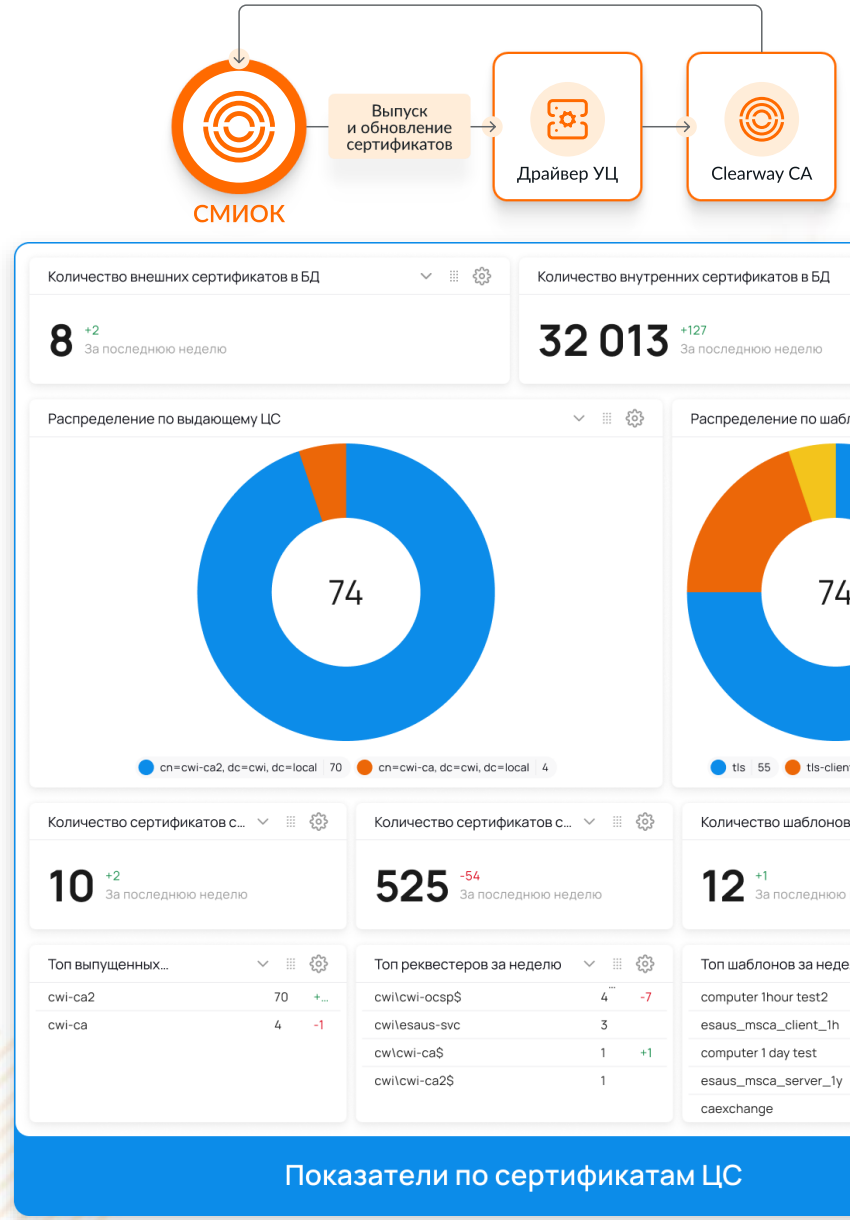
На слайде представлены основные возможности системы мониторинга инфраструктуры открытых ключей (СМИОК):

Мониторинг ИОК — поддерживается контроль состояния компонентов инфраструктуры, обеспечивающий выявление недоступности, сбоев и отклонений в работе критичных узлов.

Мониторинг сертификатов — поддерживается контроль сертификатов и шаблонов по заданным признакам, позволяющий выявлять объекты, требующие внимания с точки зрения статуса и потенциально небезопасных настроек.

Инструменты для работы с сертификатами — предоставляется набор средств для просмотра, проверки и анализа сертификатов и шаблонов, а также для выполнения операций по их обслуживанию.

В числе прочих возможностей — почтовые уведомления, статистика и отчёты, интеграция через API и многие другие возможности



Показатели по сертификатам ЦС

Интеграция с СУУ СКЗИ

СУУ СКЗИ – система управления и учета СКЗИ

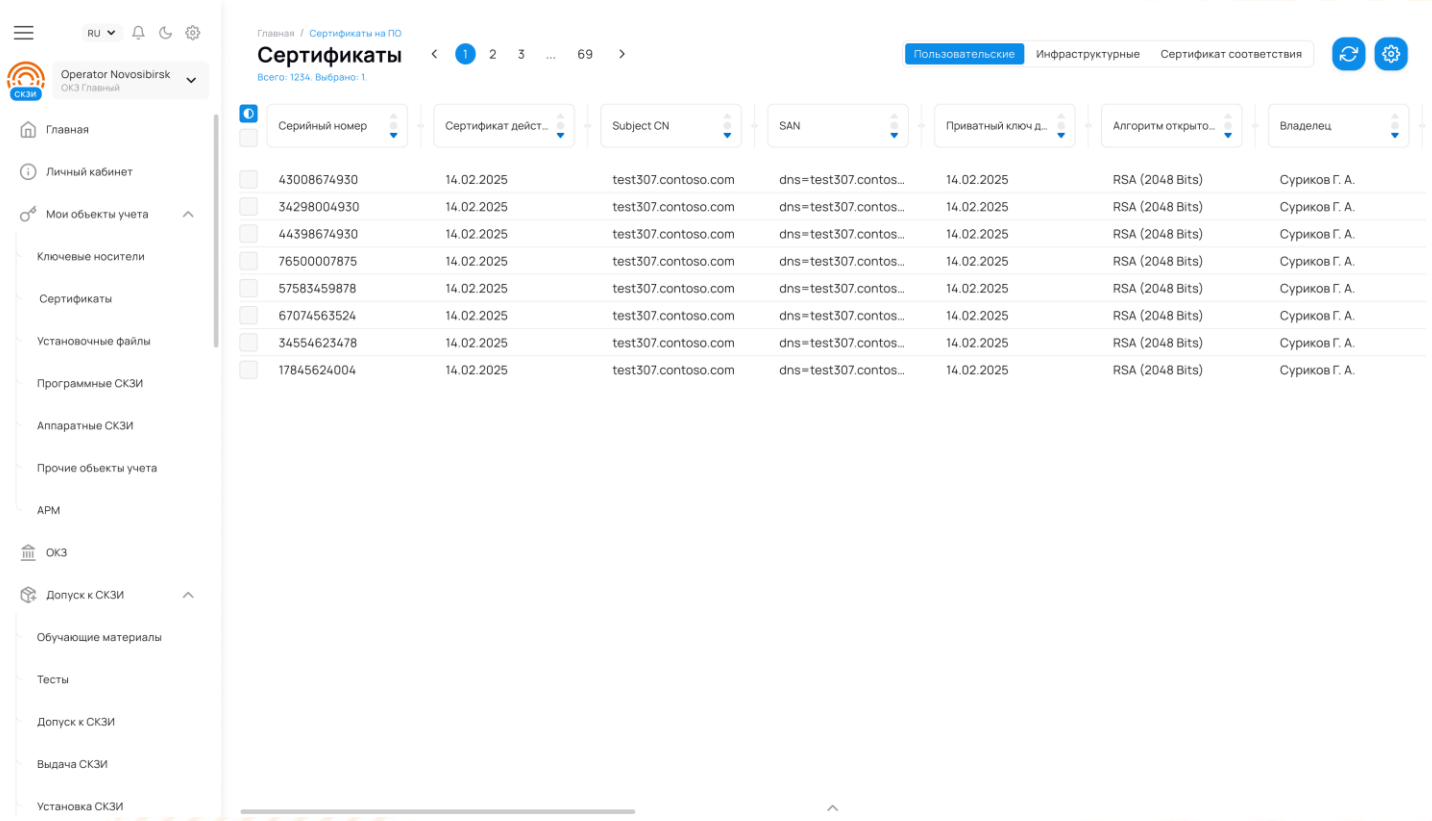
Цель интеграции – выпуск сертификатов для нужд СКЗИ

Выпуск и запись сертификатов на токены

– СУУ СКЗИ использует Clearway CA для выпуска и записи сертификатов токены пользователей;

Это позволяет обеспечить полный цикл работы с токеном:

1. Регистрация токена в системе учета
2. Выдача токена пользователю
3. Фиксация выдачи в журналах ОКЗ\ОКИ
4. Запись сертификата на токен
5. Автоматический учет и инвентаризация сертификата и токена



Интеграция с ЦУГИ EXC

EXC — централизованное решение для управления секретами.

Цель интеграции – защита паролей и ключей на ЦС

На слайде представлены основные возможности системы управления секретами (EXC):

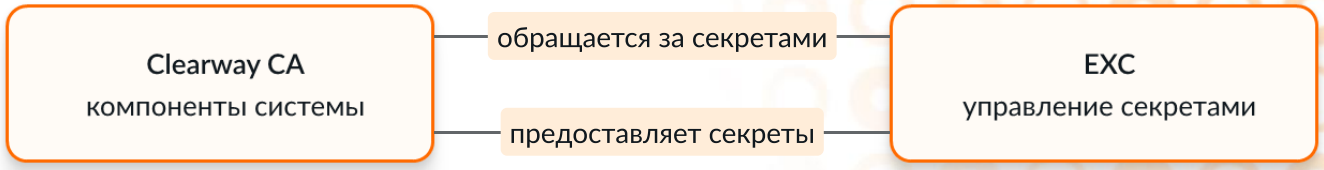
Управление жизненным циклом секретов — система берёт на себя всю работу с секретами: вовремя обновляет постоянные, выдаёт временные, когда они нужны, и убирает те, что больше не используются.

Безопасное хранение — секреты собраны в одном защищённом хранилище и всегда зашифрованы, в том числе по алгоритмам ГОСТ.

Разграничение доступа — каждый видит только то, что ему положено: доступ выдаётся по ролям, а при необходимости настраивается точнее через ACL-политики.

Доставка секретов потребителям — секреты сами попадают туда, где нужны: в контейнеры, на серверы, в инструменты CI/CD. Для устаревших систем подойдут переменные окружения и файлы конфигурации.

Clearway CA обращается к EXC за секретами, необходимыми для работы своих компонентов, — паролями доступа, данными подключения к базам данных и иными конфиденциальными параметрами.



Дорожная карта

CLEARWAY INTEGRATION

2026

1-й квартал

- Архивирование сертификатов с истекшим сроком действия;
- Графический инсталлятор для установки и первичной настройки системы;
- Интеграция с системой ЦУГИ.EXC.

2-й квартал

- Поддержка работы с КриптоПро CSP;
- Конструктор создания CSR-запросов в пользовательском интерфейсе.
- Контекстные справки по функционалу в пользовательском интерфейсе.

3-й квартал

- Расширение функциональности сервиса OCSP;
- Предотвращение ошибочных повторных выпусков сертификатов;
- Редактирование конфигурации через пользовательский интерфейс.

4-й квартал

- Обновление сертификата ЦС через мастер в графическом интерфейсе;
- API предоставления метрик в формате Grafana;
- Отдельная версия для корневых ЦС.

Лицензирование

Модули	Метрики лицензирования
Модуль автоматического формирования сертификатов и CRL для УЦ Clearway CA на базе Astra OpenSSL	Без ограничения по количеству экземпляров УЦ
Модуль графического пользовательского интерфейса Clearway CA	Без ограничения по количеству экземпляров УЦ
Функция автоматической балансировки запросов для OCSP	Без ограничения по количеству экземпляров УЦ
Модуль синхронизации CRL для УЦ и внешних точек распространения COC.	На один контур управления Без ограничения по количеству экземпляров УЦ
Модуль синхронизации сертификатов со службой каталогов Microsoft Active Directory.	На один контур управления Без ограничения числа сканируемых хостов
Модуль синхронизации сертификатов со Службой каталогов Samba	На один контур управления Без ограничения количества синхронизуемых объектов
Модуль KRA (Key Recovery Agent) и функция шифрования БД сертификатов	Без ограничения количества экземпляров УЦ
Модуль расширенных метрик мониторинга	На один контур управления Без ограничения по количеству экземпляров УЦ
Модуль автоматической проверки сертификатов по протоколу OCSP.	На один контур управления Без ограничения числа клиентов
Модуль поддержки протоколов SCEP/NDES.	На один контур управления Без ограничения числа клиентов
Модуль поддержки протоколов ACMEv2, CMP, EST	Без ограничения по количеству экземпляров УЦ
Модуль поддержки протоколов MS-WSTEP (MS-RPC)	Без ограничения по количеству экземпляров УЦ
Модуль автоматизации административных задач для УЦ	Без ограничения по количеству экземпляров УЦ
Модуль архивирования истекших сертификатов	Без ограничения по количеству экземпляров УЦ
Модуль интеграции ИОК OpenSSL с KeyBox	На один контур управления Без ограничения уникальных имен сертификатов

Техническая поддержка

Стандартная поддержка (инцидентная поддержка)

Доступна для всех владельцев действующих продуктов Clearway Integration. Эксперты Clearway Integration смогут проконсультировать, как правильно настроить ПО для решения типовых задач в рамках функциональных возможностей наших продуктов и платформенных решений.

Включает в себя:

- Реагирование на инциденты 8x5;
- Консультации по типовой настройке продукта;
- Консультации по использованию функциональных возможностей продукта;
- Предоставление периодических отчётов о результатах оказаний услуг технической поддержки.

Премиальная поддержка

Улучшенная поддержка с оптимизированным временем реагирования на инциденты. Премиальный уровень технической поддержки – это расширенный формат стандартного взаимодействия с корпоративными заказчиками, разработанный на основе лучших мировых практик.

Включает в себя:

- Реагирование на инциденты 24/7;
- Консультации по типовой настройке продукта;
- Консультации по использованию функциональных возможностей продукта;
- Диагностика ПО и предоставление временного/обходного/постоянного решения;
- Выделенный координатор технической поддержки 8x5;
- Удалённая техническая поддержка;
- Проактивная техническая поддержка.

Техническая поддержка

CLEARWAY INTEGRATION

	Стандарт	Премиум
Поддержка 8x5 с понедельника до пятницы	✓	✓
Поддержка 24/7	✗	✓
Поддержка в выходные и праздничные дни	✗	✓
Решение инцидентов и предоставление временного/обходного/постоянного решения	✓	✓
Предоставление периодических отчётов о результатах оказания услуг технической поддержки	✓	✓
Диагностика ПО и предоставление рекомендаций по дальнейшим шагам работы с системой	✗	✓
Резервное копирование компонентов продукта	✗	✓
Установка исправлений ПО ЦУГИ	✗	✓
Проведение периодических обследований и анализ статистики работы системы на основе инцидентов, логов, отчётов системы мониторинга	✗	✓
Информационно-консультационные услуги по эксплуатации продуктов	✗	✓
Информационно-консультационные услуги по эксплуатации продуктов	✓	✓
Выделенный координатор технической поддержки 8x5	✗	✓
Бесплатная диагностика инцидентов вызванных внешней инфраструктурой	✗	✓

О компании

Clearway Integration - российский разработчик ПО для управления и мониторинга Информационных систем, разработчик продуктов, помогающих повысить управляемость и информационную безопасность. Компания создает эффективные решения на базе платформы ЦУГИ, повышающие уровень безопасности и автоматизации ИТ-инфраструктуры компаний.

Clearway Integration - надежный поставщик ИТ- и ИБ-продуктов отечественной разработки для импортозамещения иностранных решений.