CLEARWAY INTEGRATION

Важна ли технологическая ИОК для информационной безопасности банка?

Автоматическое обновление и установка технологических сертификатов

Секция:
«PKI в кредитно-финансовом секторе»

CLEARWAY INTEGRATION

Почему технологический ИОК важен ИБ?

Особенности Тех. ИОК

- Часто управляются ДИТ
- Криптография RSA и мин. ГОСТ
- Админ отвечает за ключи своей ИС
- Админ сам формирует CSR
- Закрытые ключи плохо защищены
- Используется для SSL/(m)TLS/IPsec/802.1x
- Выполняет функцию AuthN/AuthZ для ИС
- Фрагментированная среда доверия
- Зоопарк версий и настроек
- Тех. сертификатов ОЧЕНЬ много
- **Почти все ИС и бизнес процессы сегодня зависят от Тех. ИОК.**

Риски Тех. ИОК

- Срок действия не под контролем
- Ошибки работы с ключами
- Нарушение зон доверия
- Нарушения области применения
- Некорректное переиспользование
- Вероятность кражи или спуфинга
- Kubernetes ISTIO использует свой УЦ
- Ошибки при установлении доверия Root
- Незакрытые уязвимости
- Ошибочные настройки
- **Тех.ИОК сильно недооценен руководителями Бизнеса, ИТ и ИБ.**

Таким образом, тех. ИОК напрямую влияет на КИИ, общую защищенность и надежность ВСЕХ бизнес-процессов любой организации.

CLEARWAY INTEGRATION

Примеры громких аварий с технологическим ИОК

КЕЙС 1

SpaceX Starlink outage caused by expired ground station certificates

8 апреля 2023 года в работе SpaceX Starlink произошёл глобальный сбой из-за просроченных сертификатов наземных станций. Пользователи по всему миру более чем на два часа остались без доступа к спутниковому Интернету, так как их абонентские устройства не получали сигналы от наземных станций Starlink

КЕЙС 2

Spotify's failure to renew security certificate causes massive podcast outage

31 мая 2022 года пользователи платформы Spotify более восьми часов не могли получить доступ к своим любимым подкастам. Сбои в работе системы возникли из-за того, что компания не смогла вовремя обновить сертификат безопасности Megaphone (одного из сервисов подкастов Spotify).

Работа крупных инфраструктур требует установки защищенных соединений, использующих TLS сертификаты как для защиты внутренних коммуникаций между компонентами сервисов и отдельными сервисами, так и для доступа клиентов.

CLEARWAY INTEGRATION

Задачи технологических ИОК - основные

- Формирование ключевой пары (функция крипто-провайдера)
- Формирование запроса CSR, сбор сведений о потребителе
- Проверка CSR на соответствие требованиям организации
- Доставка CSR до удостоверяющего центра
- Выпуск сертификата на УЦ
- Обеспечение надежности и производительности ИОК
- Доставка сертификата до Потребителя
- Установка и актуализация сертификата у Потребителя
- Своевременная замена устаревшего сертификата

CLEARWAY INTEGRATION

Задачи ИОК - вспомогательные

- Учет технологических окон при выполнении обновления сертификатов
- Актуализация списка доверенных корневых сертификатов
- Распространение информации об отозванных сертификатах CRL, OCSP и другие методы
- Логирование выпуска, установки и обновления сертификатов.
- Мониторинг состояния и функций ИОК
- Мониторинг срока действия сертификатов и ключей
- Уведомления владельцев сертификатов о сроке или отзыве
- Анализ статистики выпуска сертификатов, выявление пиковых нагрузок
- Личный Кабинет для Пользователей Сертификатов
- Механизмы оперативного отзыва сертификатов и удаления связанного с ними ключевого материала
- Безопасное обращение с ключевым материалом
- Поддержка краткосрочных сертификатов в Kubernetes ISTIO Service Mesh, сценариях Network Access Control/Network Access Protection
- Оперативное отслеживание сроков действия и фактов отзыва внешних сертификатов
- Инвентаризация фактического использования сертификатов
- Единый Справочник Сертификатов организации и полнотекстовый поиск в нем
- Резервное копирование и восстановление ИОК или отдельных ее компонентов
- Контроль за исполнением персоналом задач по обслуживанию ИОК
- Поддержка сложно сегментированных сетей
- Проверка актуальности версий установленных крипто-провайдеров и крипто-библиотек
- Балансировка нагрузки и автоматическое переключение между несколькими однотипными УЦ
- Поддержка и динамический выбор УЦ от разных производителей

CLEARWAY INTEGRATION

Что могут популярные готовые решения?

Функция	SCEP	ACME v2	CMP и EST	Microsoft Enterprise PKI
Доставка сертификата до потребителя	+	+	+	+
Установка и актуализация сертификата у потребителя	-	-	-	+/-
Своевременная замена устаревшего сертификата	-	-	-	+/-
Сбор расширенных сведений о потребителе	-	+/-	+/-	+
Обеспечение надежности и производительности ИОК	-	+	+	+
Актуализация списка доверенных корневых сертификатов	-	-	+	+
Распространение информации об отозванных сертификатах	-	-	+/-	+
Мониторинг состояния и функций ИОК	-	-	-	+/-
Мониторинг срока действия сертификатов и ключей	-	-	-	+/-
Безопасное обращение с ключевым материалом	+	+	+	+
Резервное копирование и восстановление ИОК	-	-	-	+
Балансировка нагрузки и переключение между однотипными УЦ	-	+	+	+
Поддержка сложно сегментированных сетей	-	-	-	+/-

CLEARWAY INTEGRATION

Опыт автоматизации технологического ИОК

Единая Система Автоматического Управления Сертификатами - предназначена для комплексного удобного контроля и управления TLS-сертификатами.

CLEARWAY INTEGRATION

Компоненты решения

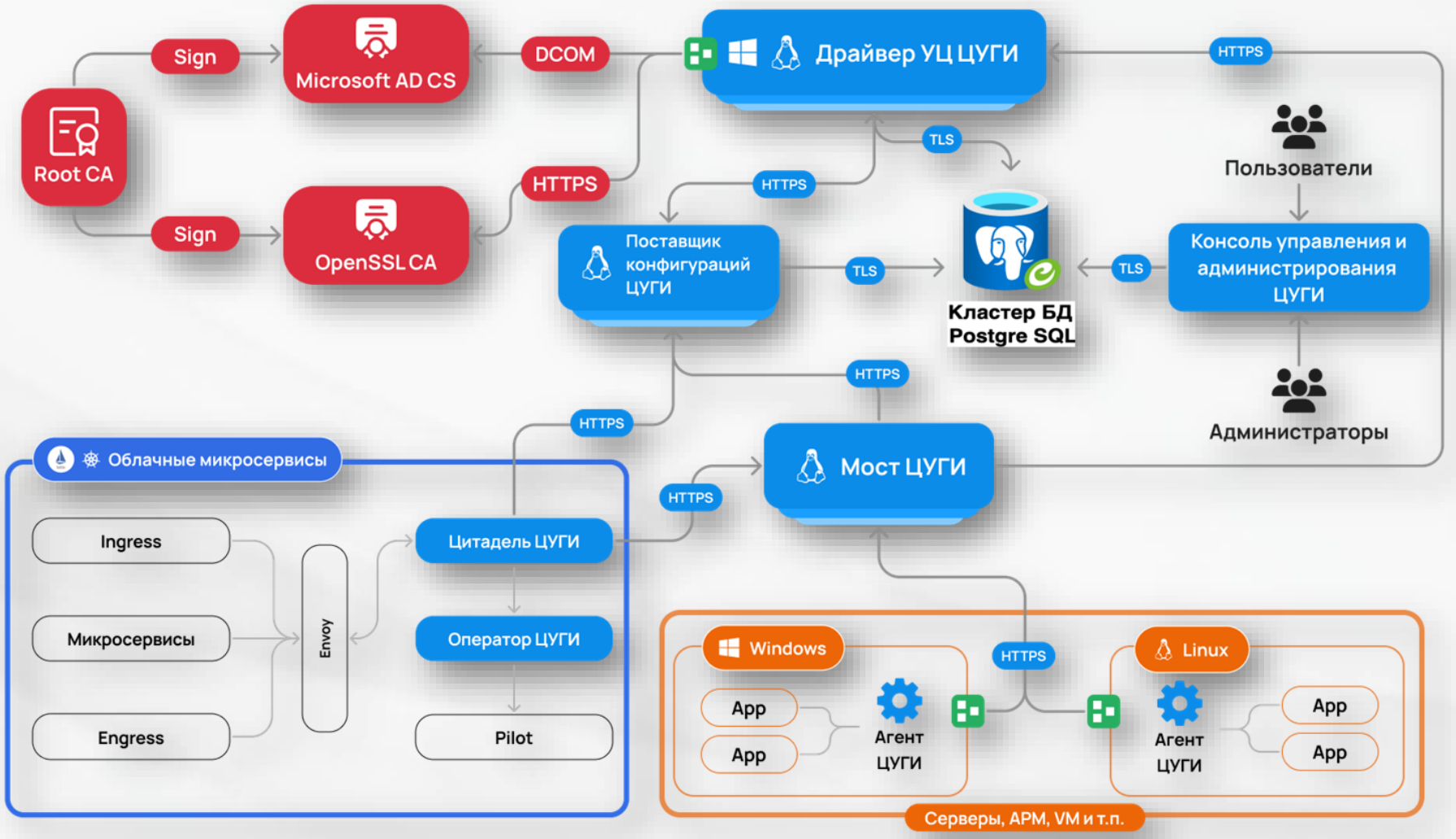
Платформа ЦУГИ (№13033 в реестре отечественного ПО)

- **Кроссплатформенный агент (Ready for Astra) – Win/Linux/AIX/MacOS**
- **Мосты (Ready for Astra)**
- **Сервер Управления Политиками и Агентами**
- **Драйвер УЦ для интеграции**

- Продукт ЕСАУС – Единая Система Автоматического Управления Сертификатами
- Агент для Windows и Linux, операторы для Kubernetes
- Замена УЦ Microsoft на Astra Linux Open SSL + сервисы ЦУГИ
- Интеграция с кластером УЦ КриптоПро
- Интеграция с KeyBox
- Интеграция с Kubernetes ISTIO
- Интеграции с прикладными и инфраструктурными ИС > 100
- Встраивание в Бизнес-Процесс развертывания новых ИС

CLEARWAY INTEGRATION

Архитектура ЕСАУС и ее компоненты



CLEARWAY INTEGRATION

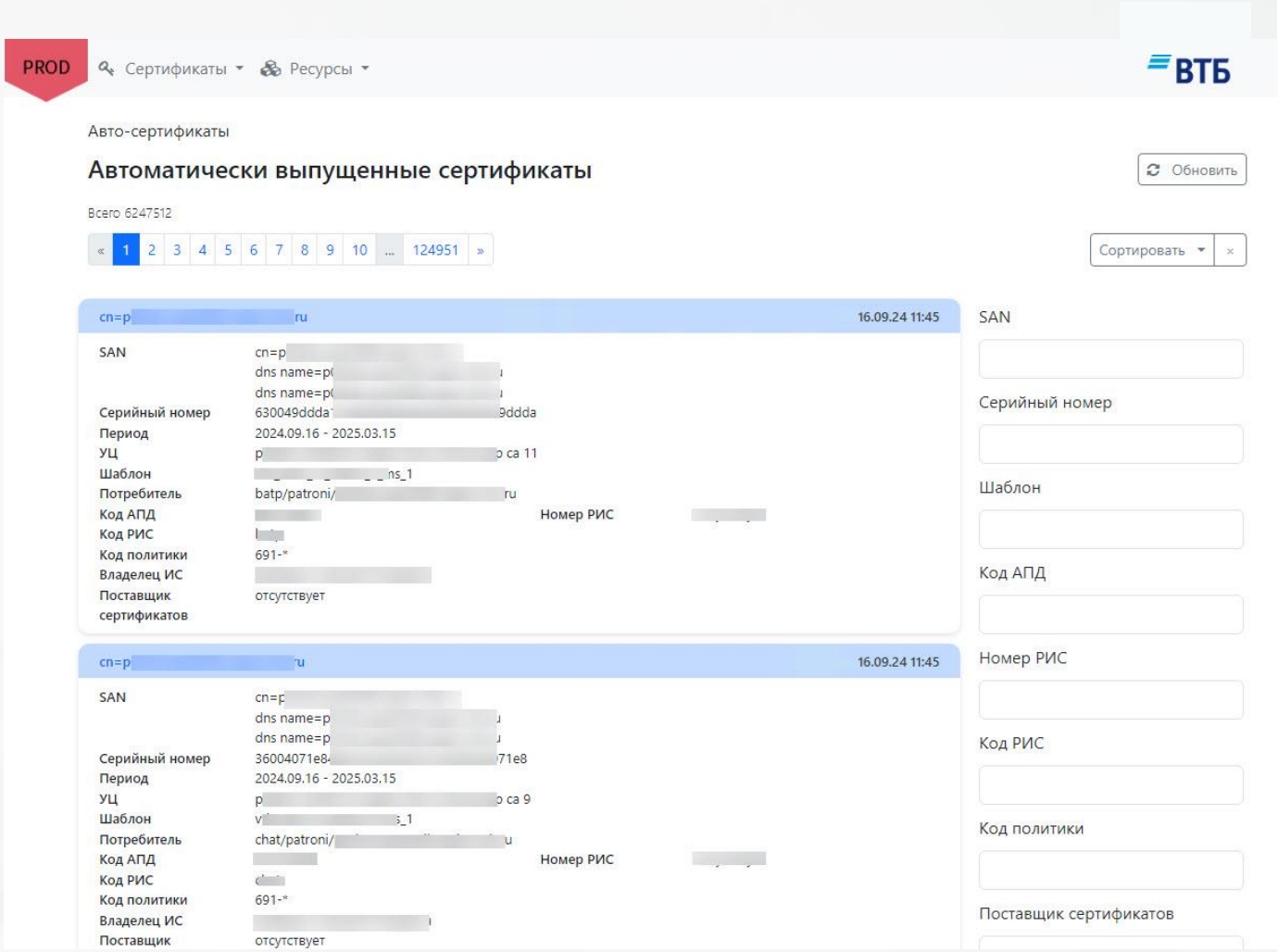
Решенные задачи

- Доставка сертификата до Потребителя через Мосты и Агентов
- Поддержка APM, серверов и контейнеров Kubernetes Istio
- Установка и актуализация сертификата у Потребителя
- Мониторинг и своевременная замена устаревших сертификатов
- Балансировка нагрузки на УЦ и высокая надежность (два плеча)
- Ролевая модель разделения задач и информации
- Отслеживание ответственности за сертификаты
- Поддержка технологических окон при обновлении сертификатов
- Установка и обновление доверенных корневых сертификатов
- Аналитика выпуска и использования сертификатов
- Связь ИС с сертификатами и ответственными
- Уведомления владельцев/ответственных за сертификаты о событиях ЖЦ

CLEARWAY INTEGRATION

ЕСАУС в цифрах

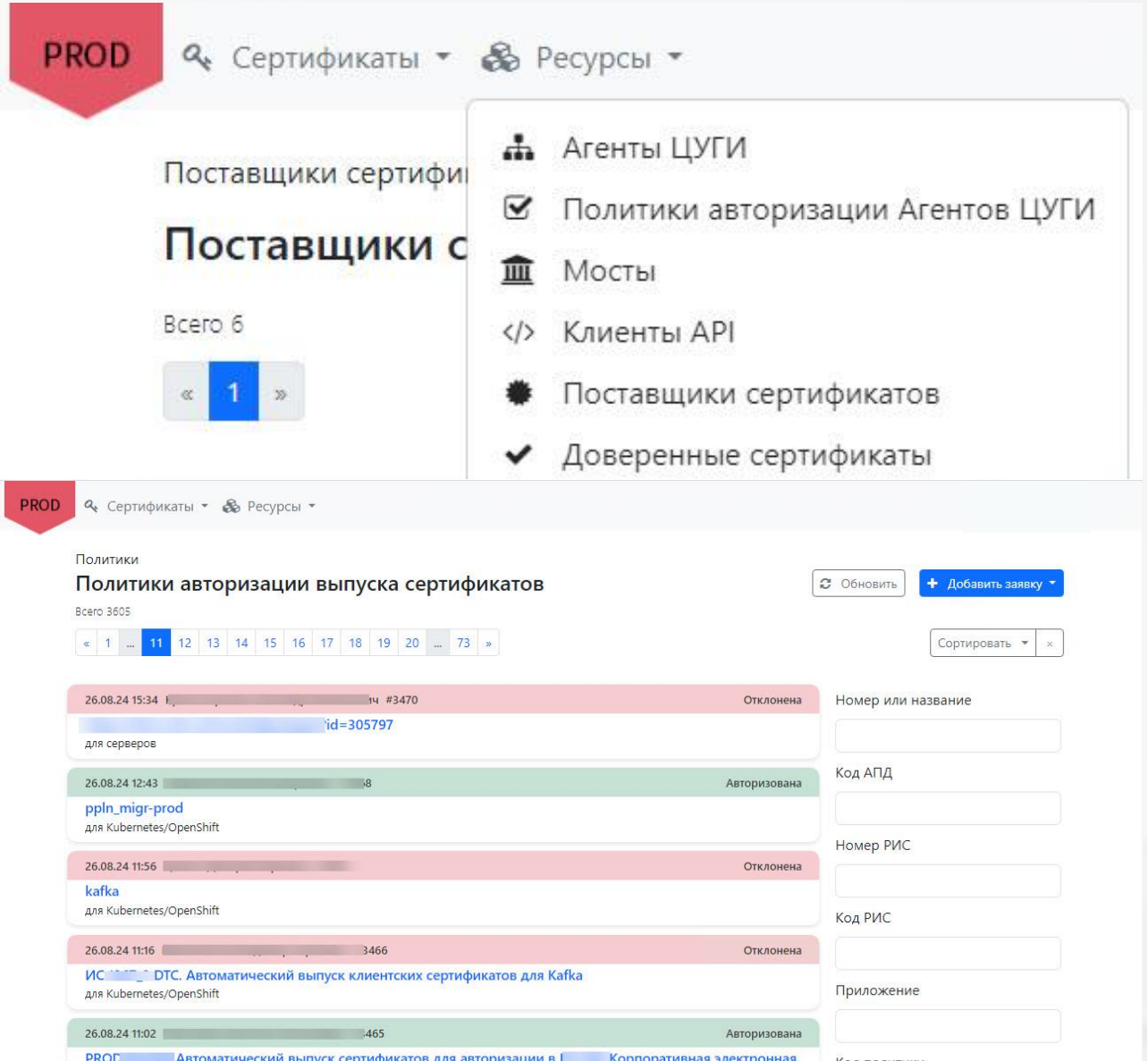
- Всего выпущено сертификатов – 30 миллионов
- Сертификатов для серверов – 10 миллионов
- Сертификатов для Kubernetes Istio – 20 миллионов
- Сертификатов для СУБД – 200 тыс.
- Пиковые нагрузки в реальной среде:
  - В рабочий день выпускается – 137 тыс.
  - В час – 16 тыс.
  - Минута – 1550 шт.
  - До 120 сертификатов в секунду



CLEARWAY INTEGRATION

Продукты и решения, интегрированные с ЕСАУС

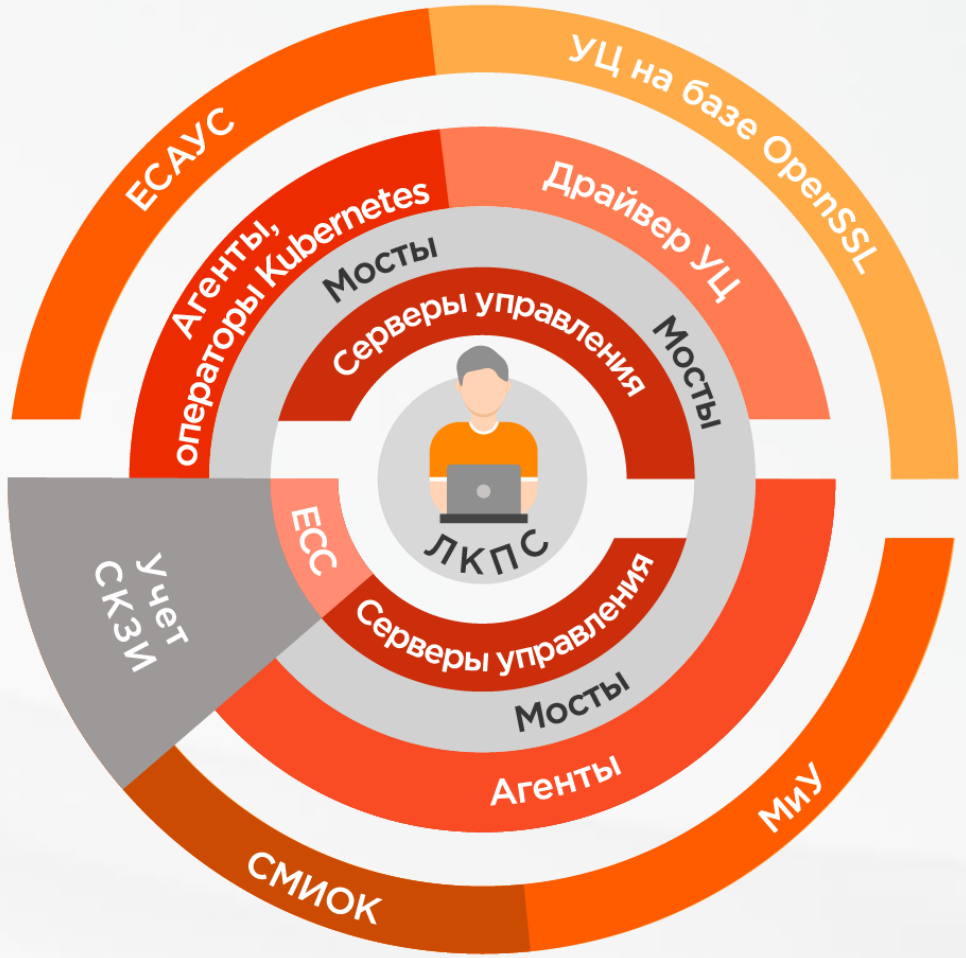
- Kubernetes/ Openshift / Istio
- PostgreSQL (+patroni)
- ETCD
- OpenSearch
- Clickhouse
- Artemis MQ
- Rabbit MQ
- Airflow
- Nginx
- Wildfly
- IBM MQ
- S3 /Ceph
- Arenadata
- Apache Kafka



CLEARWAY INTEGRATION

Экосистема решений платформы ЦУГИ

- **ЕСАУС** – предназначена для комплексного и удобного контроля и управления TLS-сертификатами
- **УЦ на базе OpenSSL** – альтернатива Microsoft Standalone CA
- **Драйвер УЦ** – позволяет работать с УЦ разных производителей.
- **Учет СКЗИ** – система осуществляет сопровождение всего жизненного цикла ключей в организации.
- **СМИОК** – обеспечивает мониторинг как самой ИОК так и внешних/внутренних сертификатов, тестирование CRL.
- **ЕСС** - объединяет сертификаты из разных источников в единую базу
- **ЛКПС** – вместе с ЕСС позволяет работать в одном окне со любыми сертификатами и СКЗИ всей организации.
- **МиУ** – система управления конфигурацией в гетерогенных ИТ-инфраструктурах, предоставляющая ИТ-службам и подразделениям ИБ инструментарий для контроля и управления различными аспектами жизненного цикла и конфигурации рабочих станций и серверов на базе ОС Linux и Windows в едином, наглядном и универсальном интерфейсе.



CLEARWAY INTEGRATION

Получите готовое решение

Москва, улица Магистральная 4-я, д. 11

clearwayit.com

info@clearwayintegration.com

+7(495)142-13-15