МИЛЛИОН СЕРТИФИКАТОВ

Как мы выпускаем и мониторим сертификаты для TLS в масштабах Банка ВТБ

CLEARWAY INTEGRATION

TECHNOLOGY. TALENT. RESULT.

Актуальные задачи

Шифрование трафика между приложениями и системами

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в статьи 14 и 14[1] Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 5 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации»

Принят Государственной Думой 6 июля 2022 года

Одобрен Советом Федерации 8 июля 2022 года

Статья 1

Внести в Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196; 2013, № 23, ст. 2870; № 52, ст. 6961; 2015, № 1, ст. 84; 2018, № 1, ст. 66; № 27, ст. 3956; № 30, ст. 4546; 2019, № 52, ст. 7798; 2021, № 1, ст. 18; № 27, ст. 5094; Российская газета, 2022, 1 июля) следующие изменения:

1) часть 5[1] статьи 14 изложить в следующей редакции:

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

- Современные системы становятся все более распределенными: переход к микросервисам, кластеризация, перенос приложений в контейнерные среды и облака
- Необходимо шифровать чувствительные данные при передаче по сети
- Требования регуляторов (ФСТЭК России, ФСБ России, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь), Роскомнадзор, Банк России, Отраслевые министерства, Межведомственные комиссии)

Драматическое увеличения числа выпускаемых сертификатов для mTLS

CLEARWAY INTEGRATION

Актуальные риски и проблемы

PKI стала mission critical и требует доступности 24/7

- один истекший сертификат может привести к отказу всей инфраструктуры в глазах клиентов
- сбой CDP может привести к отказу жизненно важных сервисов
- нарушение границ доверия может привести к порче или хищению продуктивных данных из тестовых сред
- ошибки конфигурации ИОК создают вектор критически опасных атак: например, захват административных привилегий через SAN сертификата
- сложность современных ИОК провоцирует ошибки, связанные с «человеческим фактором»
- возникновение потребности в сертификатах с коротким сроком действия
- отзыв весной 2022 года сертификатов у подсанкционных банков

Система ЦУГИ мониторит здоровье и угрозы ИОК, автоматизирует выпуск и доставку сертификатов до потребителей на разных платформах

CLEARWAY INTEGRATION

Платформа решения для ВТБ – система ЦУГИ

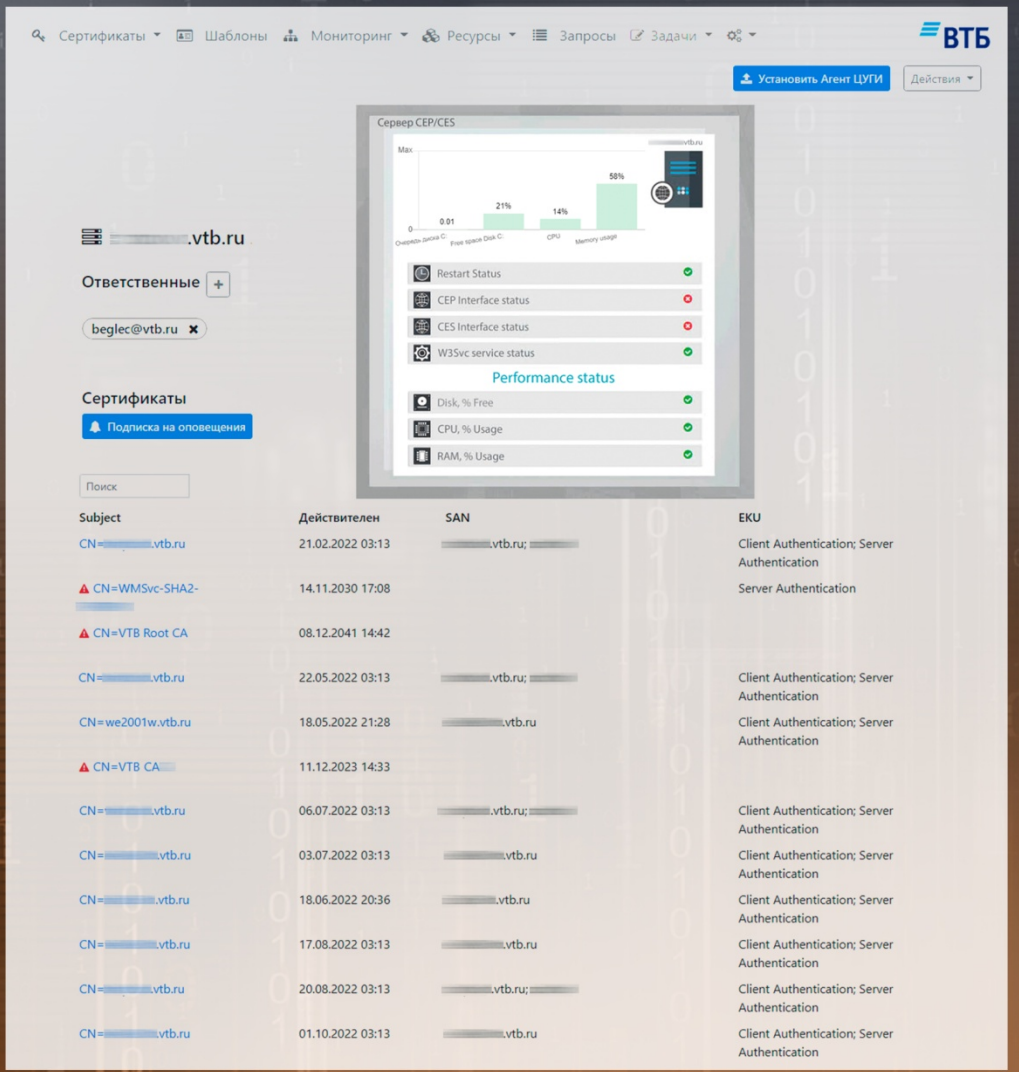
- Кроссплатформенный Агент для Windows, Linux, AIX, MacOS
- Нативная интеграция с Kubernetes, OpenShift и другими облачными средами
- Драйвер УЦ – для абстракции от УЦ разных производителей
- Мосты ЦУГИ – для сложной топологии сетей
- Универсальная расширяемая CMDB – для хранения сертификатов и других типов КЕ
- Сквозная подпись всех транзакций выпуска сертификатов
- Модули Workflow, Task Tracking, RBAC для встраивания в реальные бизнес-процессы
- Надежность и масштабируемость

CLEARWAY INTEGRATION

TECHNOLOGY. TALENT. RESULT.

Мониторинг сертификатов и PKI в ВТБ

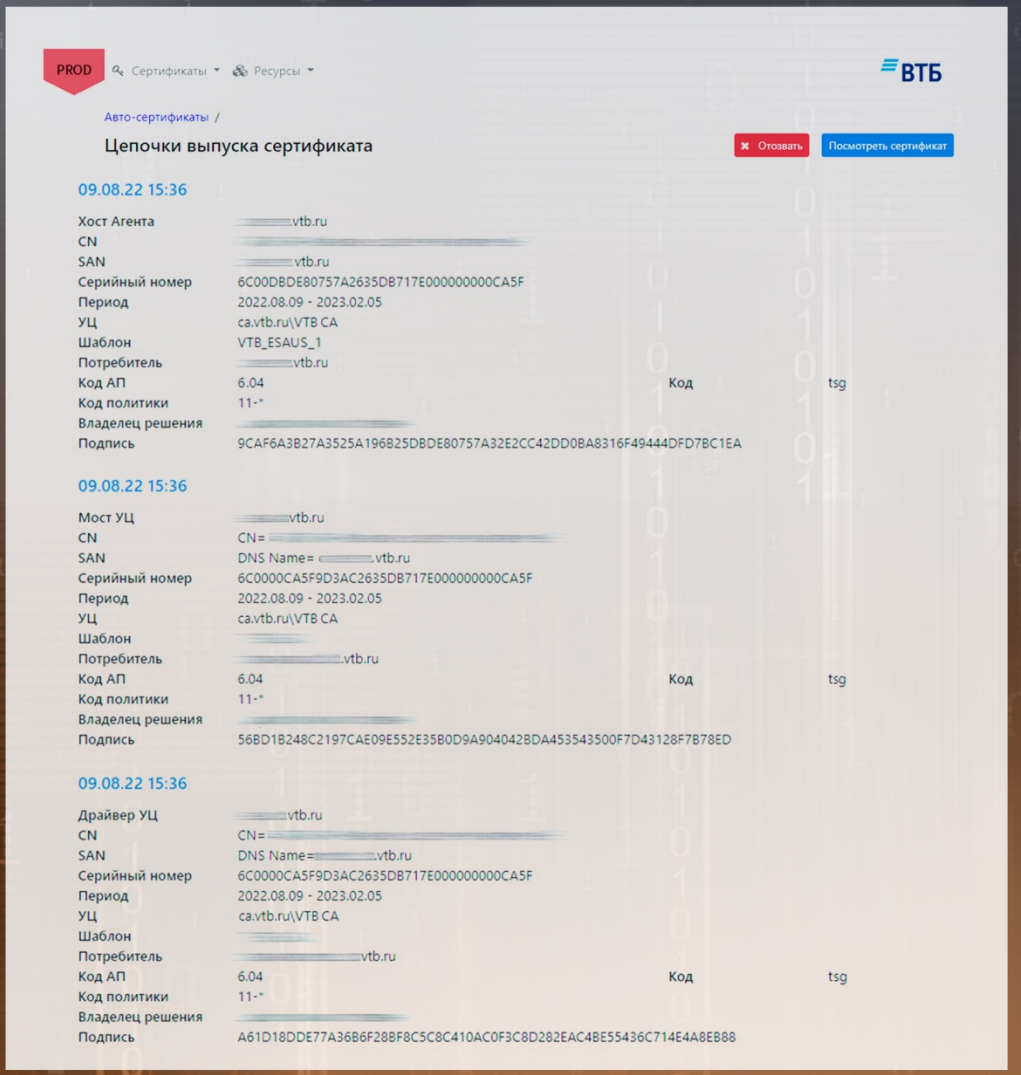
- Инвентаризация сертификатов непосредственно с УЦ, а так же агентом с серверов и АРМ
- Проверка и анализ всех загруженных в систему сертификатов по спектру рисков и потенциальных проблем
- Мониторинг HSM и сетевой доступности локальных компонентов PKI
- Загрузка в базу и мониторинг сертификатов от внешних УЦ
- Мониторинг доступности AIA, CDP, OCSP и других элементов ИОК, влияющих на выпуск сертификатов
- Поиск, фильтрация и выгрузка в Excel списков сертификатов
- Подписка на уведомления о событиях мониторинга ИОК и отдельных сертификатов



CLEARWAY INTEGRATION

Автоматизация выпуска сертификатов в ВТБ

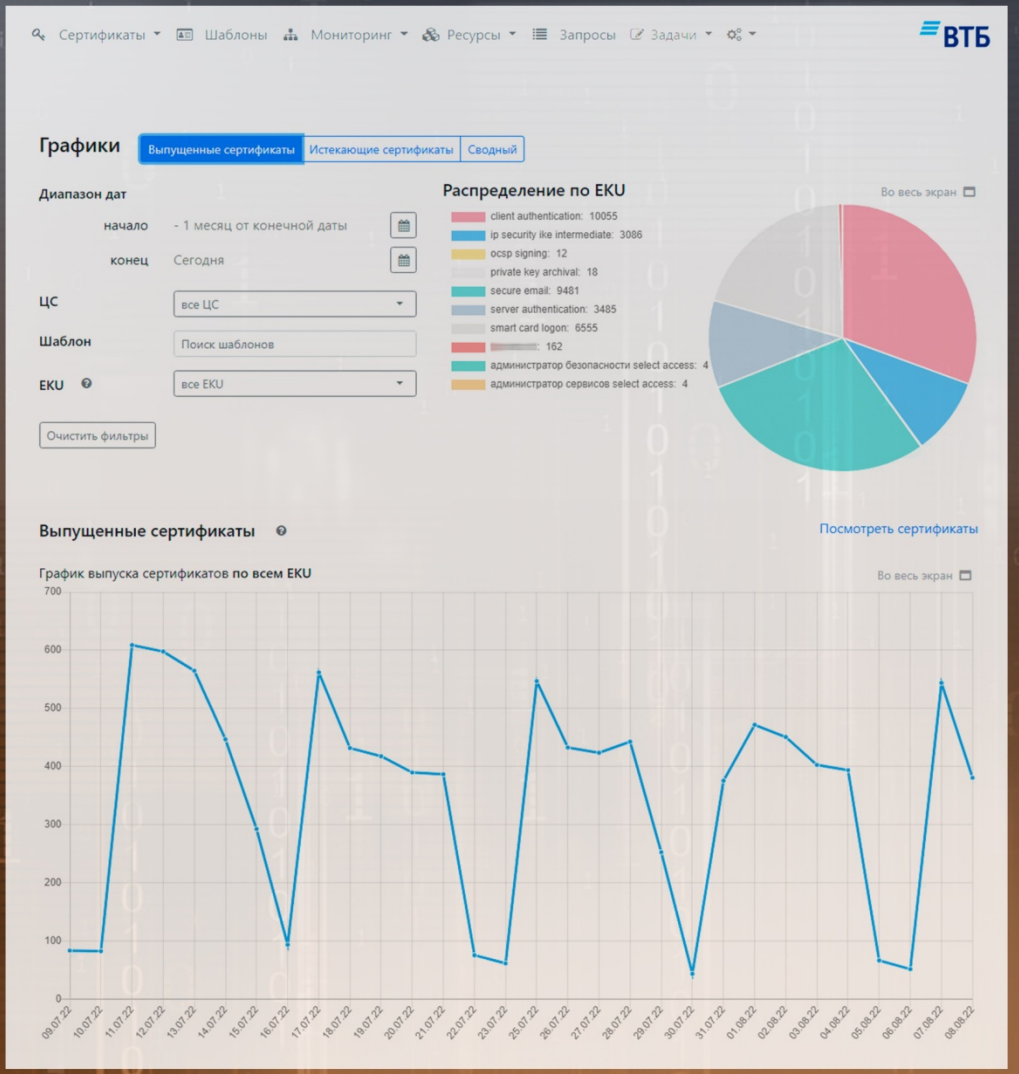
- Автоматический выпуск и обновление сертификатов во всех средах: Kubernetes, классические серверы, клиентские АРМ
- Единый реестр сертификатов для всех сред: промышленной, тестирования, разработки и др.
- Гибкие политики и механизмы утверждения заявок на выпуск сертификатов
- Интеграция с частной облачной платформой
- Автоматическое размещение сертификатов в хранилищах систем-потребителей, координация обновлений для ферм и кластеров
- Полная осведомленность о сертификате: от его заказчика до его размещения
- Самостоятельный выпуск сертификатов с подтверждением и без



CLEARWAY INTEGRATION

Аналитика и отчетность

- Графики распределения сертификатов по времени и типам
- Динамическая перестройка графиков при перенастройке и изменении фильтров
- Активные графики и отчеты – возможность перехода по клику на элементе графика в список с соответствующим множеством сертификатов
- Интеграция с Grafana и выгрузка в Excel/Мой Офис
- Интерактивные панели мониторинга с возможностью настройки силами заказчика
- Разработка интерактивных таблиц, графиков и отчетов под заказ



CLEARWAY INTEGRATION

Совместимость и интеграция

Операционные системы

- Windows 7 и новее
- Linux (RedHat, Ubuntu, AstraLinux…)
- IBM AIX, Mac OS X

Контейнерные среды

- Kubernetes
- OpenShift

Аутентификация и RBAC

- Microsoft ActiveDirectory
- Keycloak

Отчеты и аналитика

- Excel/Мой Офис
- Grafana

Выпуск сертификатов

- PostgreSQL, Microsoft SQL
- ClickHouse, ElasticSearch, Tarantool
- Kafka

- Веб-серверы: Nginx, IIS
- Серверы приложения Java: Wildfly…
- Artemis, RabbitMQ

ЦУГИ - российское ПО. Запись в реестре №13033 от 21.03.2022

О ЦУГИ в цифрах в контексте ВТБ

Инсталляции:

- Сервера управления - 3
- Мосты ЦУГИ - 20
- Драйверы УЦ - 7
- Агентов и Control plane > 2000

Обслуживание и мониторинг УЦ:

- Для сред разработки и тестирования - 2
- Для промышленных сред - 10

Выпущено сертификатов:

- 600 000 для тестовых сред
- 100 000 для сред разработки
- 300 000 для промышленной среды

CLEARWAY INTEGRATION

Спасибо за внимание!

http://clearwayintegration.com
+7(495)142-13-15
+7(968)625-10-78
info@clearwayintegration.com

CLEARWAY INTEGRATION

TECHNOLOGY. TALENT. RESULT.