

Технологический сертификат как цифровой паспорт машины

Система управления служебными
и технологическими сертификатами

Иван Черников

Руководитель продукта Рутокен CLM,
Компания «Актив»





Доверие в ИТ-инфраструктуре

Это уверенность, что:

- каждый объект инфраструктуры на самом деле является таковым
- каждый элемент имеет доступ только к той информации, которая ему предназначена
- мы можем доверять информации, получаемой от каждого объекта инфраструктуры

Доверие обеспечивается идентификацией и аутентификацией каждого элемента инфраструктуры:

- объекты (машины, микросервисы, ПО)
- субъекты (пользователи)

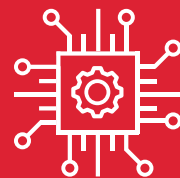


Что является факторами доверия?



Для людей:

- пароли
- ОТП
- аппаратные средства
- домены



Для машин/сервисов:

- сертификаты X.509
- mTLS соединения
- закрытые ключи

Сертификат X.509 – цифровой паспорт машины

Не путать с пользовательским СКЗИ – это другой объект с другим жизненным циклом

Что содержит?

- Публичный ключ
- Идентификатор объекта
- Срок действия
- Подпись УЦ

Где применяется?

- Аутентификация устройств
- Межсервисное взаимодействие
- Подпись кода и пакетов

Жизненный цикл:



Новые требования регулятора



С 1 марта 2026 года действует приказ №117 ФСТЭК.

В методическом документе по его реализации от 12.04.2026 перечислены требования к аутентификации устройств/сервисов в ИС (ИАФ 4).

Основные пункты:

- ✓ аутентификация должна производиться при каждом запросе на подключение устройства к ИС
- ✓ основные протоколы: CMP, EST, ACME, WSTEP, TLS (протоколы для управления сертификатами)
- ✓ смена аутентификационных данных должна происходить не реже чем один раз в год
- ✓ аутентификация устройств предполагает наличие корпоративного центра сертификации

Требуется использование системы централизованного управления жизненным циклом цифровых сертификатов!

Что происходит сейчас



Слепая зона: сертификаты как неучтённый актив

Ситуация:

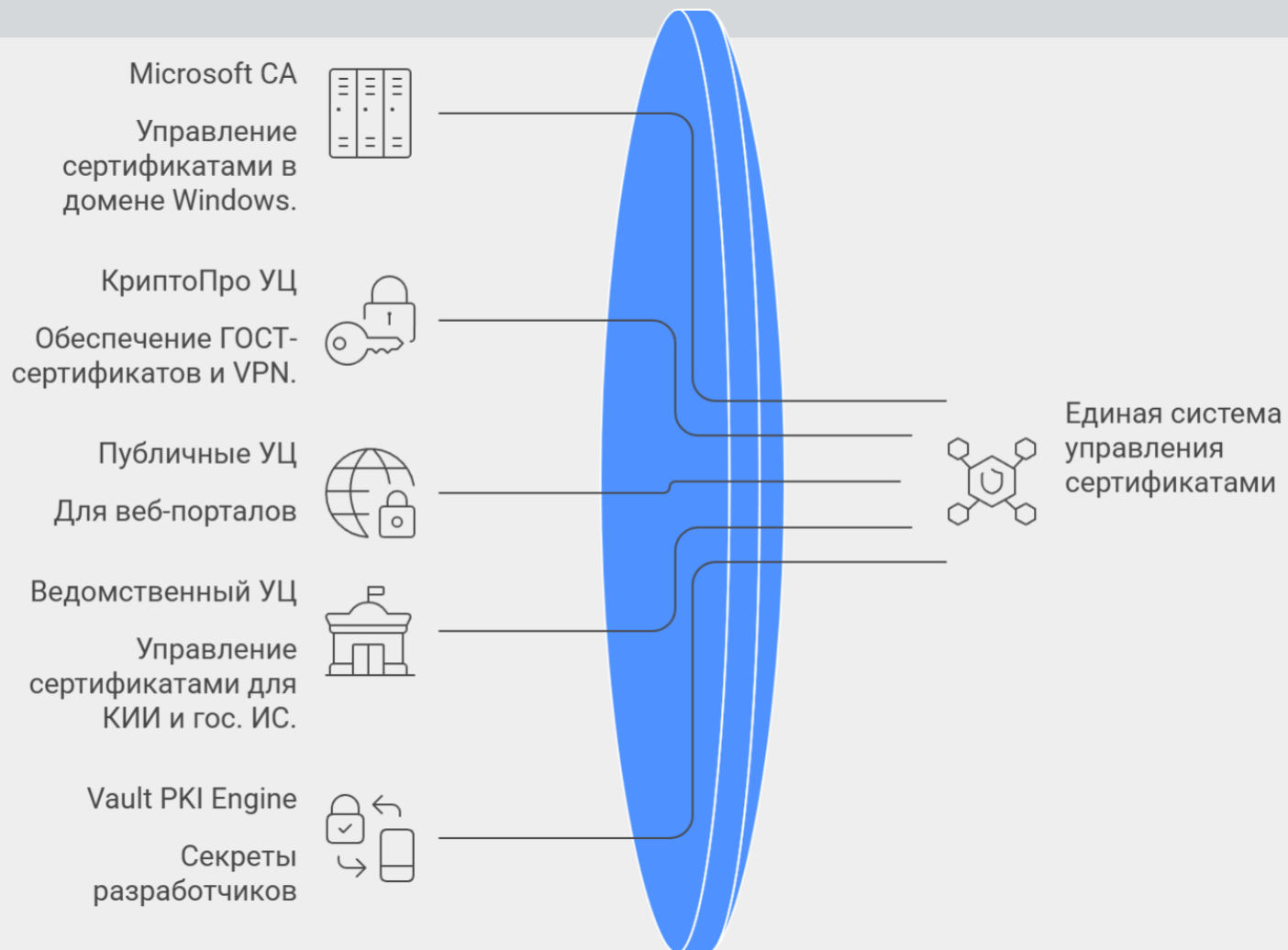
- сертификаты из разных УЦ учитываются по-разному
- сертификаты выпускаются по мере необходимости, без реестра
- Wildcard и «вечные» сертификаты покрывают десятки сервисов, никто не знает, где именно
- ответственность размыта: ИТ, Devops, разработка
- истечение сертификата = сбой сервиса + уязвимость в периметре



96%

организаций вручную
управляют сертификатами

Разнообразие УЦ



Как это должно работать?

Нужное решение

Для полного контроля
над инфраструктурой нужны:

- ✓ сканирование инфраструктуры и поиск сертификатов
- ✓ единое окно для мониторинга и управления сертификатами
- ✓ сценарии автоматического обновления и развертывания.



Сканирование

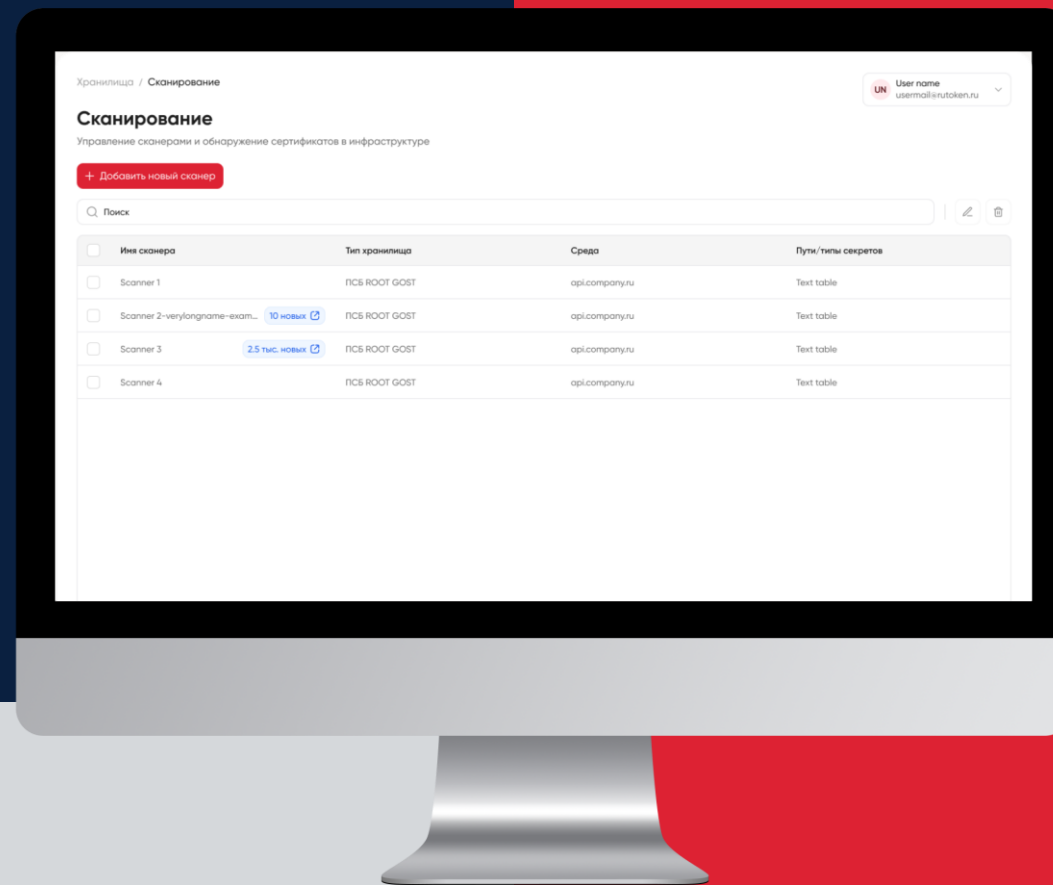


Ядро системы — реестр сертификатов

- Агентская схема сканирования
- Гибкая периодичность проверок
- Сканеры для отдельных зон или всей инфраструктуры
- Автоматическое добавление новых сертификатов в реестр

В будущих версиях планируется:

безагентское сканирование сертификатов от публичных УЦ (Global Sign, Letsencrypt) по доменным именам.



Автоматизация

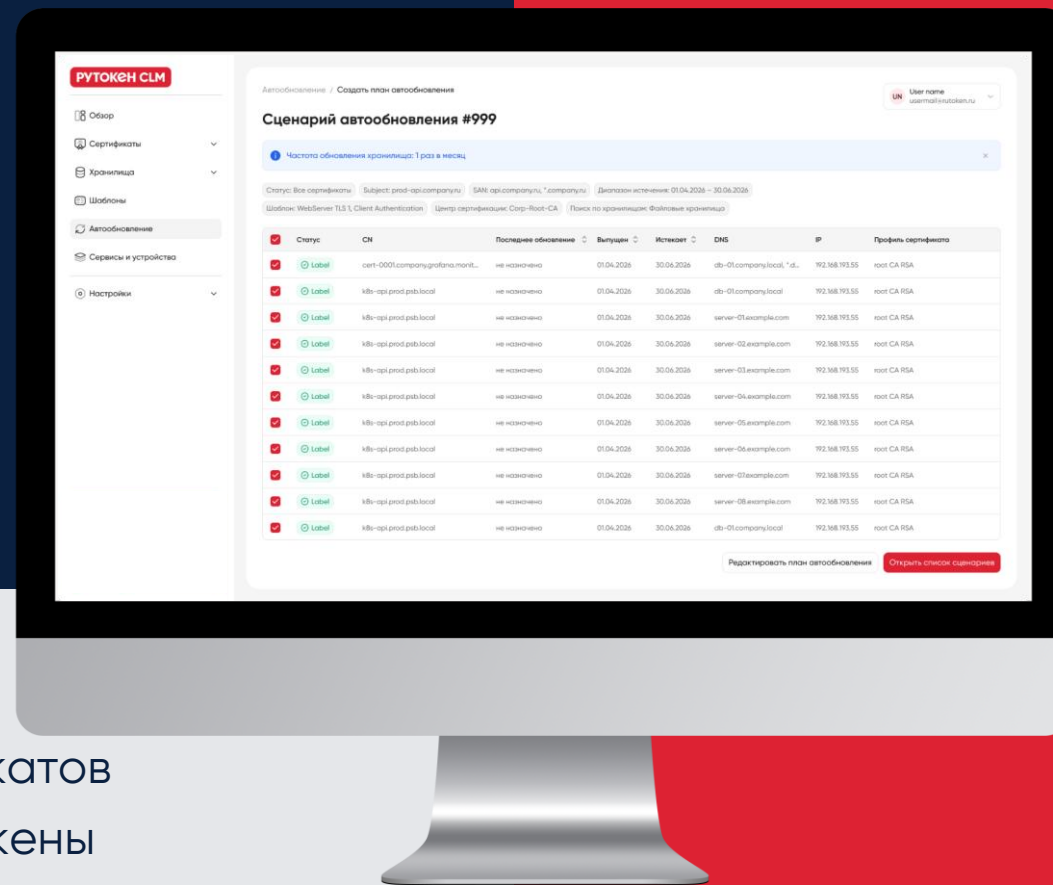


Планы автоматизации

- Гибкий график обновления
- Логирование всех действий с сертификатами
- Выпуск новых ключей на хостах
- Перезапуск сервисов после обновления
- Поддержка разнообразия хранилищ и сертификатов

В будущих версиях планируется:

- расширение списка обновляемых сертификатов
- поддержка новых типов хранилищ: HSM, токены
- автоматизация обновления пользовательских сертификатов



Обзор

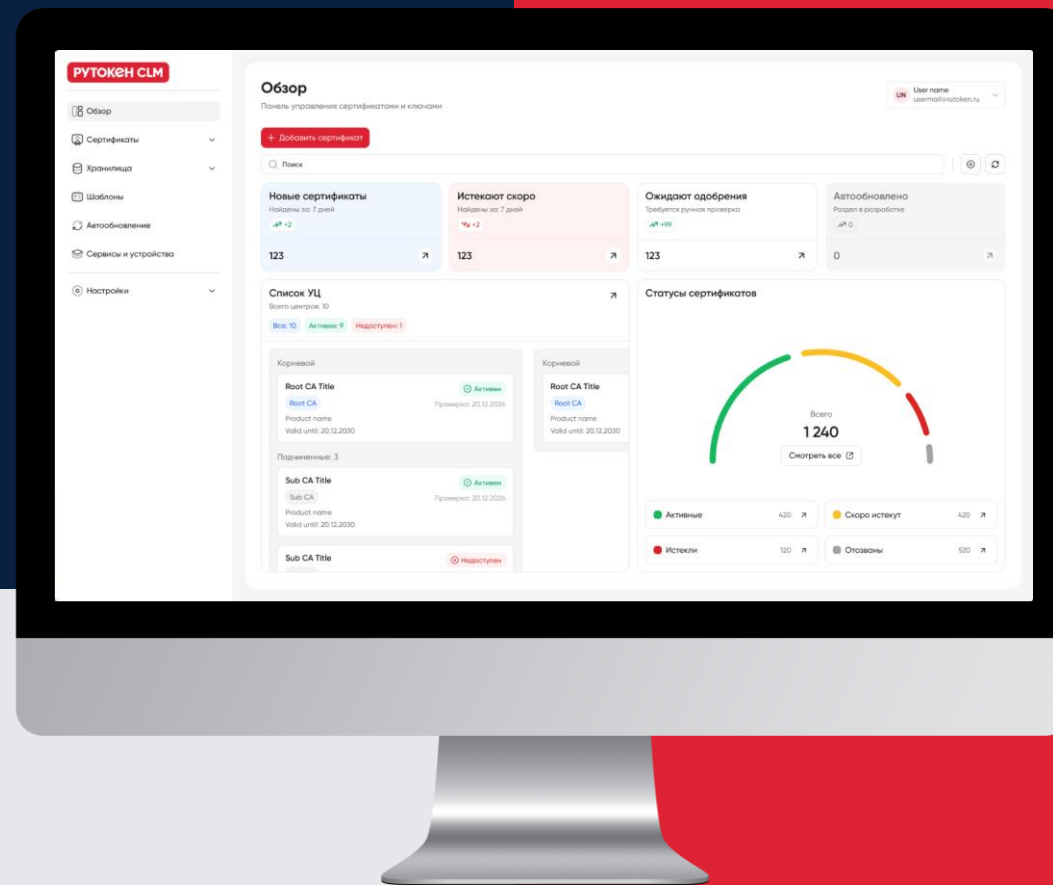


Дашборд

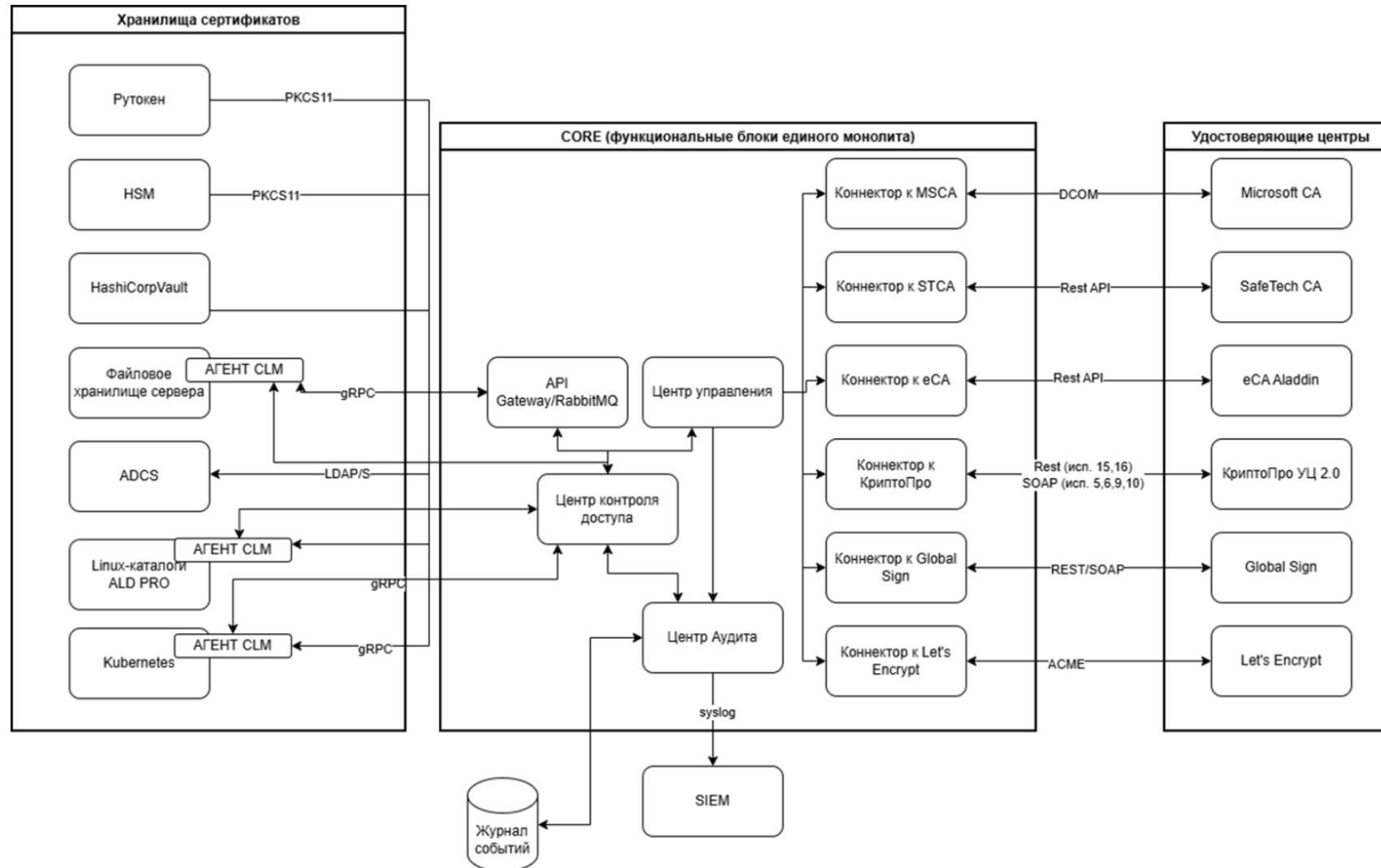
- Количество и расположение сертификатов
- Цепочка центров сертификации
- Контроль сроков истечения
- Возможность аудита
- Уведомления об истечениях, инцидентах

В будущих версиях планируется:

- настройка и кастомизация дашборда
- подтягивание информации из систем управления СКЗИ



Структура продукта



Лучшая практика



Регулярно проверять систему, проводить аудит для обеспечения безопасности

6



Внедрить систему автоматизации

5



Устранить выявленные уязвимости и риски

4



Провести первичную инвентаризацию

3



Установить четкие правила и процедуры для работы с сертификатами

2



Назначить ответственного и зону владения

1





Чеклист проверки по ИАФ 4

Checklist



- ✓ Есть ли реестр устройств и сервисов, использующих сертификаты?
- ✓ Каков срок действия каждого сертификата?
- ✓ Как организована смена аутентификационных данных раз в год?
- ✓ Какой УЦ выпускает сертификаты для устройств?
- ✓ Кто контролирует истечение и отзыв?



Без системы CLM ответить на эти вопросы документально невозможно!

Команда **продукта**



Иван Черников

Руководитель продукта Рутокен CLM,
Компания «Актив»



ich@aktiv-company.ru
info@rutoken.ru



www.rutoken.ru
www.aktiv-company.ru



+7 925 421-02-61

РУТОКЕН

