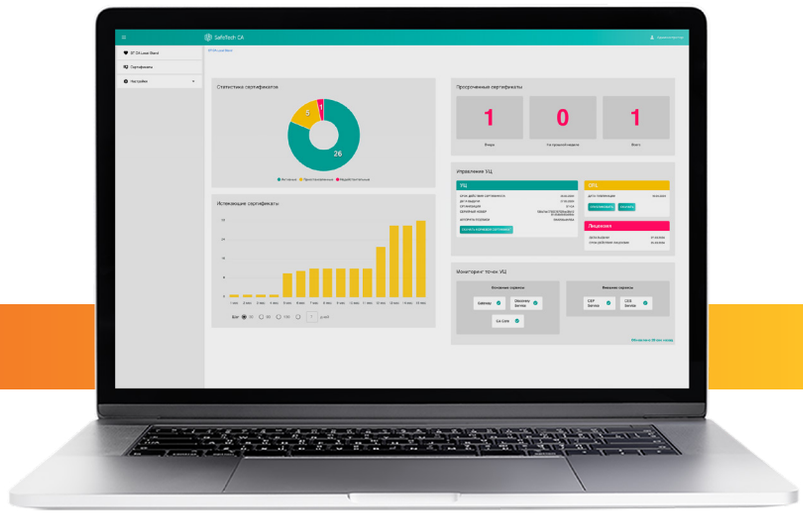
SAFETECH
SAFETY TECHNOLOGIES



SafeTech CA

Современный корпоративный центр сертификации, способный не только полностью заменить Microsoft CA, но и значительно оптимизировать процессы выпуска и управления жизненным циклом сертификатов, сделав их более удобными и эффективными.

Продукт позволяет снизить риски приостановки работы Microsoft CA на территории РФ и выполнить требования законодательства по импортозамещению:

- Указ Президента РФ от 30.03.2022 № 166
- Указ Президента РФ от 01.05.2022 № 250
- Указ Президента РФ от 07.05.2018 № 214
- Приказы Министерства цифрового развития № 334 от 04.07.2017 и № 335 от 04.07.2018
- Постановление Правительства РФ № 1236 от 16.11.2015

В SafeTech CA можно легко и привычно:

- выпускать технологические сертификаты и управлять их жизненным циклом
- применять как зарубежную (RSA, ECDSA, EDDSA), так и отечественную криптографию (ГОСТ)
- проверять статус сертификата как через сеть точек CRL, так и online через OCSP
- создавать иерархию PKI, добавляя корневые/промежуточные/выпускающие CA
- размещать ключи CA во внешних HSM
- и многое другое.

Современный отечественный центр сертификации

ПРЕИМУЩЕСТВА

ИМПОРТОЗАМЕЩЕНИЕ

Реализация протокола MS-WSTEP и интеграция с Microsoft Active Directory позволяют заменить Microsoft CA и обеспечить безопасный autoenrollment-сервис на полностью отечественном ПО.

ЛИЧНЫЙ КАБИНЕТ ПОЛЬЗОВАТЕЛЯ

Простой и понятный web-интерфейс добавляет гибкости организации бизнес-процессов по управлению сертификатами, предоставляя пользователю инструмент для самостоятельного формирования запросов, отслеживания статуса их согласования, выгрузки выпущенных сертификатов и ключей и т.д.

УНИВЕРСАЛЬНОСТЬ ПРИМЕНЕНИЯ

Поддержка протоколов MS Enrollment и SCEP позволяет выпускать сертификаты для обширного перечня сетевого оборудования и различных устройств, работающих на разных операционных системах (Windows, Linux, Mac, iOS, *nix-системы).

УВЕДОМЛЕНИЯ ОБ ИЗМЕНЕНИИ СТАТУСА СЕРТИФИКАТА

Гибко настраиваемые администратором правила уведомлений позволяют оперативно и своевременно информировать пользователя об изменении статуса сертификата.

БЕСШОВНАЯ МИГРАЦИЯ С MICROSOFT CA

Механизм импорта шаблонов и сертификатов из Microsoft CA помогает осуществить миграцию быстро и легко, без длительного периода параллельной работы двух сервисов и ожидания истечения срока действия сертификатов, выпущенных Microsoft CA.

ПОДДЕРЖКА ГОСТ-КРИПТОГРАФИИ

Возможность работы с сертификатами не только на базе зарубежных, но и российских ГОСТ-криптоалгоритмов значительно упрощает управление PKI-инфраструктурой, избавляя от необходимости использовать несколько центров сертификации под разные процессы.

О КОМПАНИИ

SafeTech — российский разработчик современных решений в области информационной безопасности, которые позволяют заказчикам создать собственный центр сертификации и автоматизировать все процессы управления инфраструктурой открытых ключей.

ПРОИЗВОДИТЕЛЬНОСТЬ И ОТКАЗОУСТОЙЧИВОСТЬ

Механизм автоматического отслеживания расположения, доступности и состояния микросервисов позволяет создавать любые отказоустойчивые конфигурации и решать задачи кластеризации в крупных территориально распределенных ИТ-инфраструктурах.

ГИБКОСТЬ И МАСШТАБИРУЕМОСТЬ

Микросервисная архитектура обеспечивает горизонтальную и вертикальную масштабируемость и дает возможность размещать дополнительные сервисы в различных сегментах.

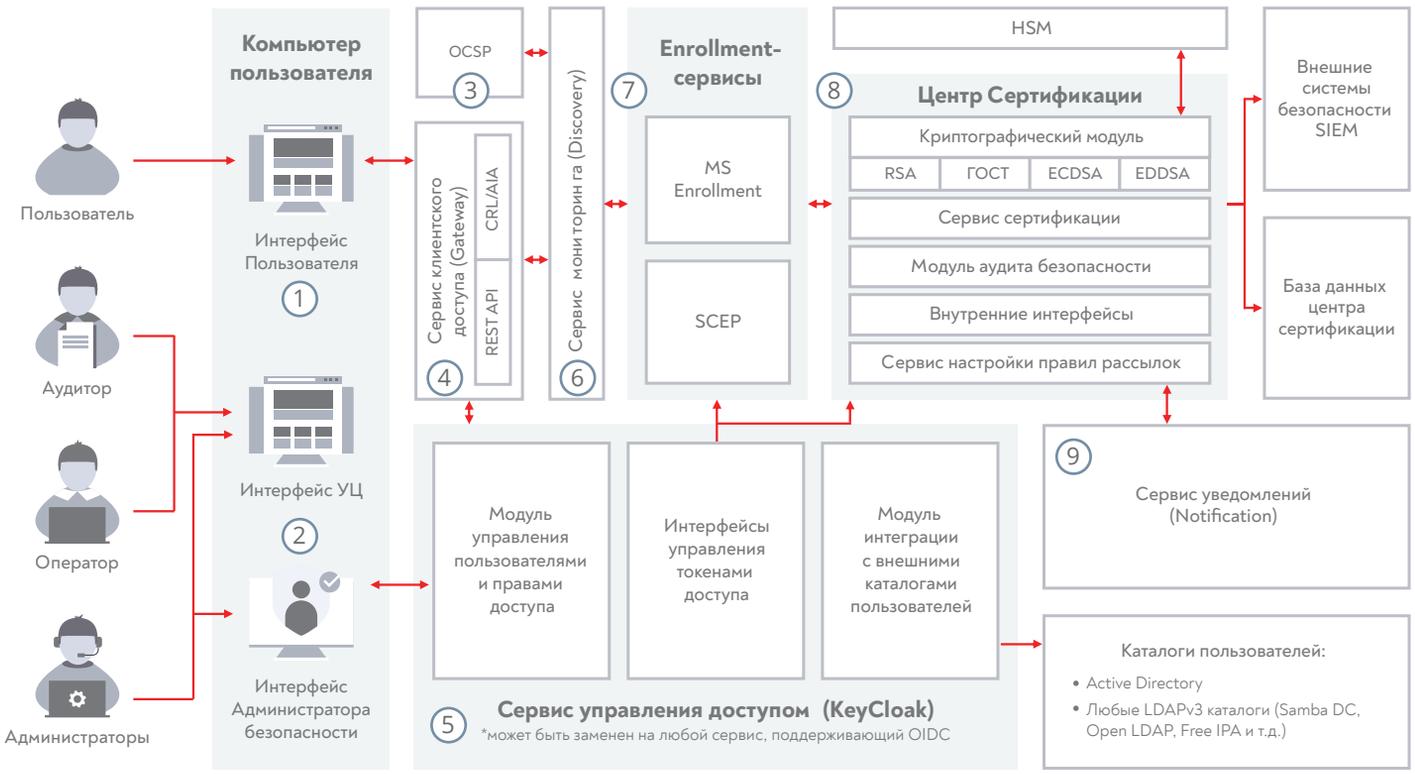
УДОБСТВО И ФУНКЦИОНАЛЬНОСТЬ ИНТЕРФЕЙСА

Расширенный функционал и наглядные дашборды дают дополнительные возможности по управлению сертификатами, в том числе, для реализации массовых операций с ними, получения статистики и выгрузки настраиваемых отчетов о выпущенных сертификатах, а также визуализации данных о доступности микросервисов.

НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ

- Поддержка современных фреймворков и технологий, таких как Spring Security, OpenID Connect, WS-Trust и т.д.
- Ролевая модель разграничения доступа (включая поддержку базовых ролей: Администратор, Оператор, Аудитор ИБ и т.д.)
- Поддержка OAuth OIDC, включая возможность использования внешних систем безопасного доступа и каталогов субъектов
- Аудит и журналирование событий безопасности, поддержка трансляции событий во внешние системы обеспечения ИБ (SIEM, IPS/IDS)
- Поддержка размещения ключей центра сертификации во внешних HSM (в том числе и для ГОСТ)

АРХИТЕКТУРА СИСТЕМЫ



ОСНОВНЫЕ КОМПОНЕНТЫ

1. **Интерфейс Пользователя**
Web-интерфейс. Обеспечивает самообслуживание пользователей (формирование запросов на сертификаты, отслеживание статуса их согласования и т.д.).

2. **Интерфейс Администратора УЦ / Оператора УЦ**
Web-интерфейс. Обеспечивает настройку, управление жизненным циклом сертификата, получение статистики центра сертификации и информации о текущем состоянии микросервисов.

3. **OCSP-сервис**
Предоставляет возможность выполнить проверку статуса сертификата в online-режиме.

4. **Сервис клиентского доступа**
Отвечает за подключение всех типов клиентов, обеспечивает маршрутизацию запросов между сервисами системы. Обеспечивает внешние интерфейсы.

5. **Сервис управления доступом**
Выполняет аутентификацию и авторизацию пользователей, а также управление пользователями и их ролями.

6. **Сервис мониторинга**
Агрегирует информацию о подключенных микросервисах, реализует механизмы балансировки нагрузки между несколькими экземплярами одного и того же сервиса.

7. **Enrollment-сервисы**
Обеспечивают выпуск и автоматический перевыпуск сертификатов для пользователей MS Active Directory, компьютеров MS Windows, Cisco-устройств, MacOS/iOS и прочих *nix-систем.

8. **Центр сертификации**
Основной компонент, ядро SafeTech CA. Обеспечивает выпуск сертификатов, работу с криптографией, взаимодействие с базой данных.

9. **Сервис уведомлений**
Реализует отправку и получение уведомлений по событиям в системе.

SafeTech
safe-tech.ru

Тел.:
+7 (495) 120-99-09

e-mail:
info@safe-tech.ru