SAFE TECH LAB

SafeTech CA

КОРПОРАТИВНЫЙ ЦЕНТР СЕРТИФИКАЦИИ

Современный корпоративный центр сертификации, способный полностью заменить Microsoft CA для Windows-инфраструктур, а также эффективно решать задачи выпуска и управления технологическими сертификатами для Linux-систем, мобильных устройств на iOS/Android, сетевого оборудования Cisco и других компонентов ИТ-ландшафта.

ПРИМЕНЕНИЕ

- VPN сервисы
- Аутентификация пользователей
- Доменные сервисы
- E-mail
- Взаимодействие оборудования
- Шифрование данных
- Mutual TLS (mTLS)
- И многое другое

ВОЗМОЖНОСТИ

- Выпуск и управление жизненным циклом сертификатов (полнофункциональный Autoenrollment в Windows/Linux)
- Поддержка зарубежной (RSA, ECDSA, EdDSA) и отечественной криптографии (ГОСТ) на базе КриптоПро CSP
- Удобный web-интерфейс администрирования и личный кабинет пользователя
- Поддержка согласования в процессе выпуска сертификатов
- Настраиваемые email-рассылки уведомлений
- Создание иерархии PKI: добавление корневых/промежуточных/выпускающих CA
- Встроенные инструменты миграции с MS CA (шаблоны, сертификаты)
- Поддержка хранения ключей CA в HSM
- Сеть точек публикации CRL/AIA, а также OCSP
- Мониторинг состояния инстанса CA и его компонентов online в web-интерфейсе ЛК
- Формирование отчетности
- Наличие REST API, поддержка стандартных enrollment-протоколов

ПЛАТФОРМЫ

- Операционные системы:
- Мобильные устройства:
- Сетевое оборудование (стандарт IEEE 802.1x)
- Другие платформы

ПРОТОКОЛЫ

MS-WSTEP
полноценная замена Microsoft CA

ACME
TLS для веб-порталов, Kubernetes, Openshift

SCEP
работа с MacOS, iOS, Android, Linux, Cisco

EST
системы MDM

SSH
сертификаты для безопасного удаленного доступа

CMP
базовый стандарт для API OpenSSL, Bouncy Castle, Nexus и других

ПРЕИМУЩЕСТВА

ИМПОРТОЗАМЕЩЕНИЕ

Глубокая интеграция с российскими операционными системами и службами каталогов на базе Linux обеспечивает безопасный Autoenrollment-сервис на полностью отечественном ПО.

минцифры_
НОМЕР В РЕЕСТРЕ: №26307

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-WSTEP 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 Lab — разработчик современных программных продуктов для построения надежной и безопасной PKI-инфраструктуры и эффективного управления ее элементами. Входит в SafeTech Group.

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.

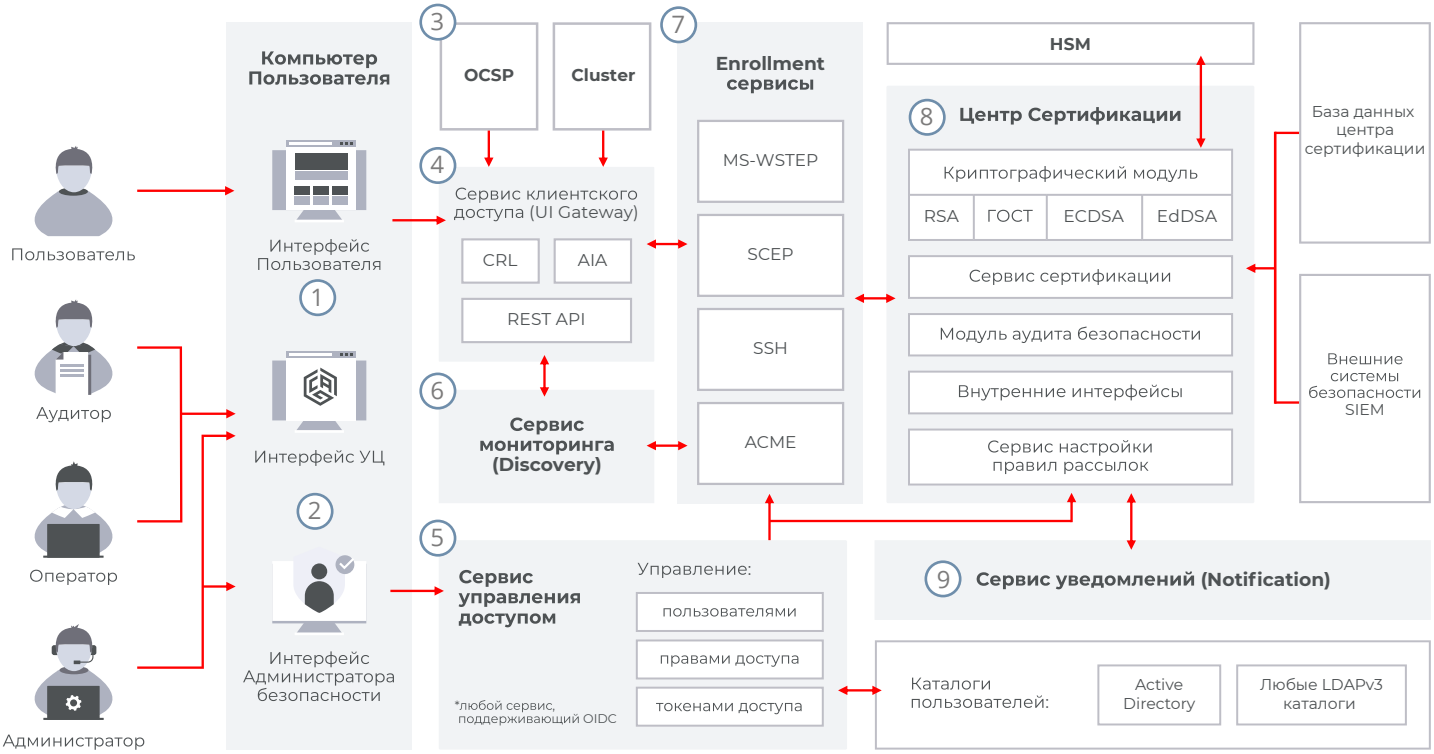
УДОБСТВО И ФУНКЦИОНАЛЬНОСТЬ ИНТЕРФЕЙСА

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 и других LDAPv3 каталогов, компьютеров MS Windows/Linux, сетевых 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 Lab
safetechlab.ru

Тел.:
+7 (495) 120-99-09

e-mail:
info@safe-tech.ru