SAFETECH
SAFETY TECHNOLOGIES

# SafeTech CA


**SafeTech CA** — современный отечественный центр сертификации, способный заменить Microsoft CA и не только. Продукт позволяет снизить риски приостановки работы Microsoft CA на территории Российской Федерации и выполнить требования законодательства по импортозамещению.

**Решение легко и привычно позволяет:**

- выпускать сертификаты и управлять их жизненным циклом
- применять как зарубежную, 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

Интеграция решения в инфраструктуру реализуется при поддержке Enrollment-сервисов и через REST API.

## КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

**Удобство и функциональность интерфейса**
Обеспечивает работу не только с базовыми функциями управлениями сертификатами, но и работу с массовыми операциями и выпуском сертификатов, получением статистики и информации о доступности микросервисов.

**Импортозамещение**
Реализует протокол Microsoft WS-Trust X.509v3 Token Enrollment Extensions (MS-WSTEP). Также SafeTech CA поддерживает интеграцию с MS ActiveDirectory.
В совокупности это делает возможным заменить Microsoft CA и обеспечить auto enrollment-сервис на полностью отечественном ПО.

**Гибкость и масштабируемость**
Микросервисная архитектура обеспечивает горизонтальную и вертикальную масштабируемость и позволяет размещать дополнительные сервисы в различных сегментах.

**Высокий уровень безопасности**

- 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)

ООО «СэйфТек»
safe-tech.ru
+7 (495) 120-99-09
info@safe-tech.ru

## ОСНОВНЫЕ КОМПОНЕНТЫ

### Центр сертификации

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

- **Криптографический модуль**
  Модель отвечает за криптографические операции, выполняемые центром сертификации. Работает как с RSA, так и с ECDSA и ГОСТ. Поддерживает возможность хранения ключей в HSM.
- **Сервис сертификации**
  Основной сервис, выполняет функции выпуска, приостановки действия, возобновления действия и отзыва сертификатов.
- **Внутренние интерфейсы**
  Модуль обеспечивает внутреннее взаимодействие и предоставляет ряд внутренних API.
- **Модуль аудита безопасности**
  Модуль отвечает за аудит и логирование событий безопасности и действий администраторов и пользователей SafeTech CA. Модуль поддерживает возможность отправки событий во внешние SIEM-системы.

### Сервис клиентского доступа

Отвечает за подключение всех типов клиентов к CA, обеспечивает маршрутизацию запросов между сервисами SafeTech CA. Обеспечивает внешние интерфейсы CA:

- **CRL Distribution Point**
  Точки распространения списка отозванных сертификатов (CRL)
- **Authority Information Access**
  Точка распространения информации о центре сертификации (AIA) REST-интерфейсы для выпуска сертификатов и управления системой

### OCSP-сервис

Предоставляет возможность выполнить проверку статуса сертификата в online-режиме.

### Сервис мониторинга

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

### Интерфейс Администратора УЦ / Оператора УЦ

Web-интерфейс SafeTech CA, обеспечивающий функции настройки, управления жизненным циклом сертификата, получения статистики центра сертификации и информации о текущем состоянии сервисов SafeTech CA.

### Enrollment-сервисы

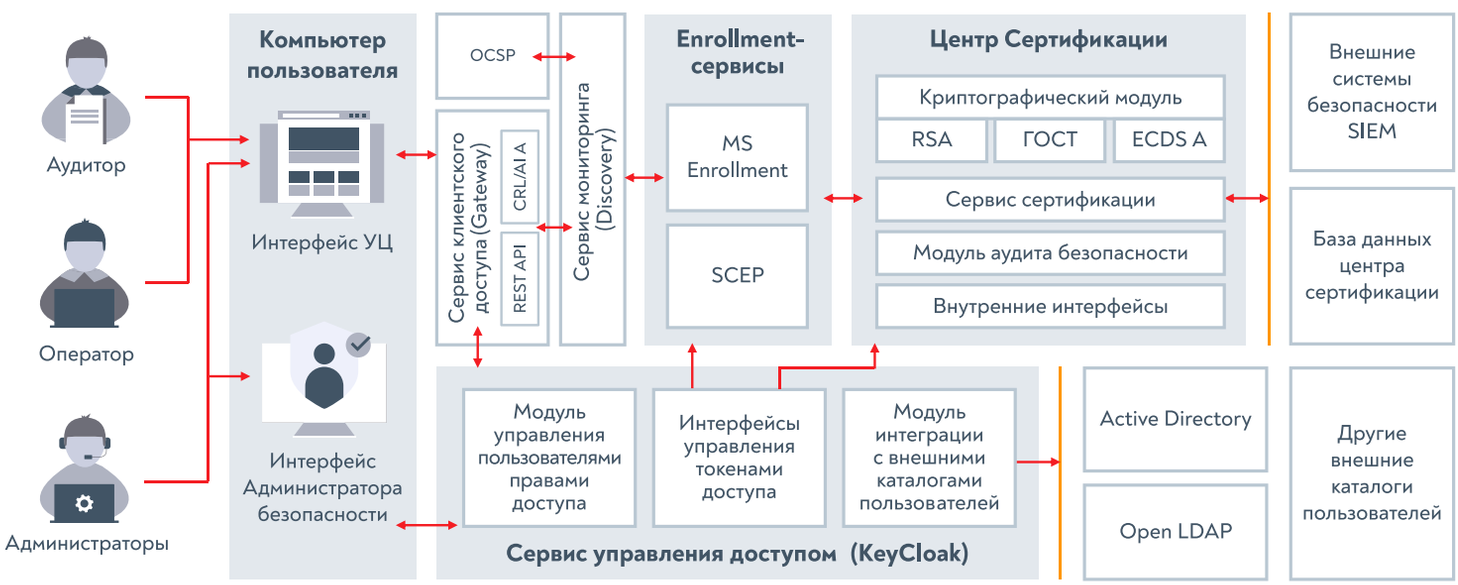
- **MS Enrollment**
  Обеспечивает поддержку выпуска и автоматического перевыпуска сертификатов для пользователей MS Active Directory и компьютеров MS Windows, реализует протокол Microsoft WSTrust X.509v3 Token Enrollment Extensions (MS-WSTEP).
- **SCEP**
  Предоставляет возможность выпуска/перевыпуска сертификатов для Cisco-устройств, MacOS/iOS и прочих *nix-систем.

### Сервис управления доступом

Сервис, выполняющий функции аутентификации и авторизации пользователей, управление пользователями и их ролями.

- **Модуль интеграции с внешними каталогами пользователей**
  Модуль выполняет функции синхронизации пользователей и их групп из внешних LDAP-каталогов, в том числе и Active Directory
- **Модуль управления пользователями и правами доступа**
  Модуль выполняет функции регистрации и управления пользователями, настройки ролей и прав доступа
- **Интерфейсы управления токенами доступа**
  Интерфейс обеспечивает методы аутентификации по протоколу OpenID Connect, методы получения и обмена токенов доступа, методы получения информации о пользователях и их ролях

## АРХИТЕКТУРА СИСТЕМЫ




## Обеспечивает выполнение требований законодательства в области импортозамещения:

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