

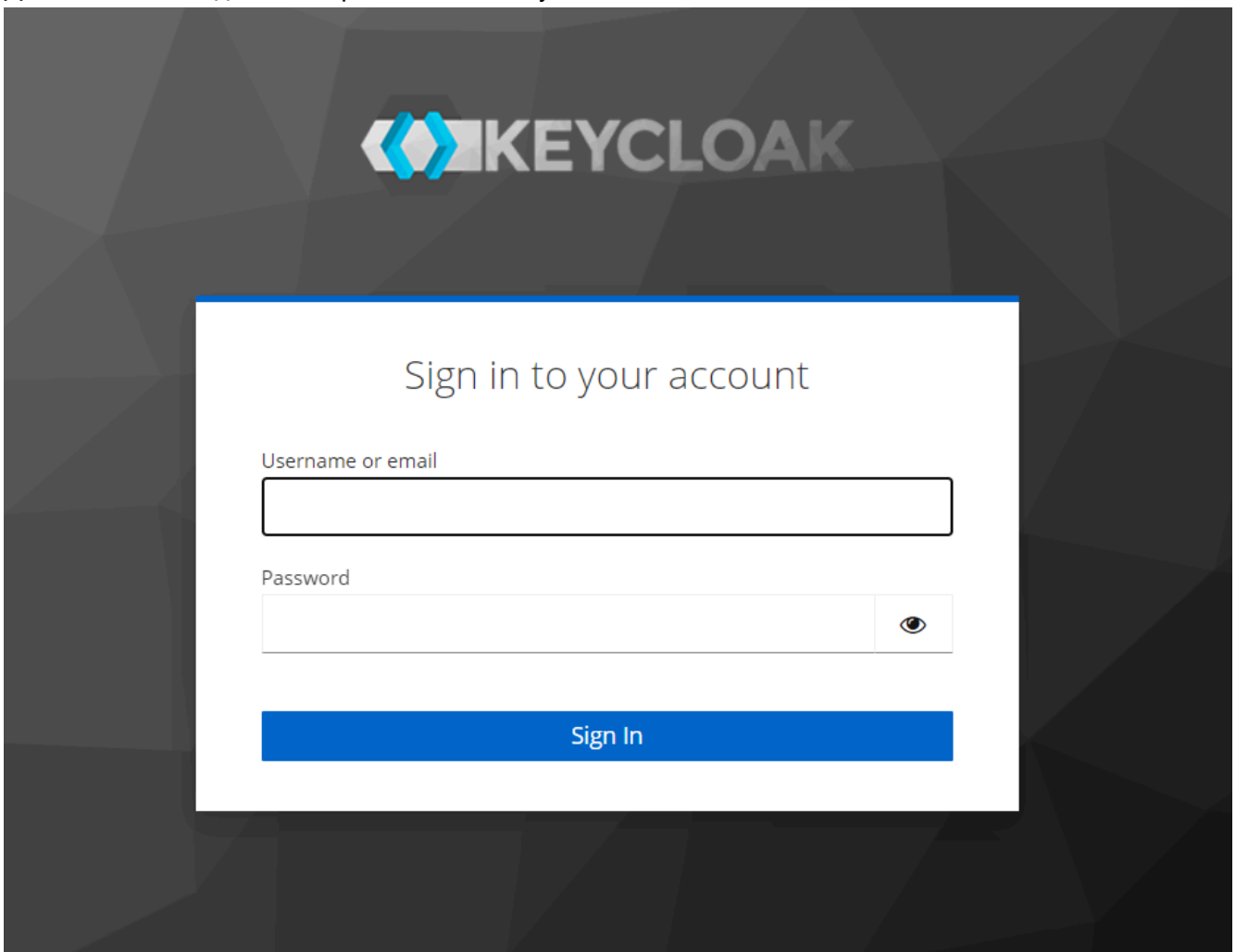
Руководство Администратора SafeTech CA 2.0

1. Авторизация

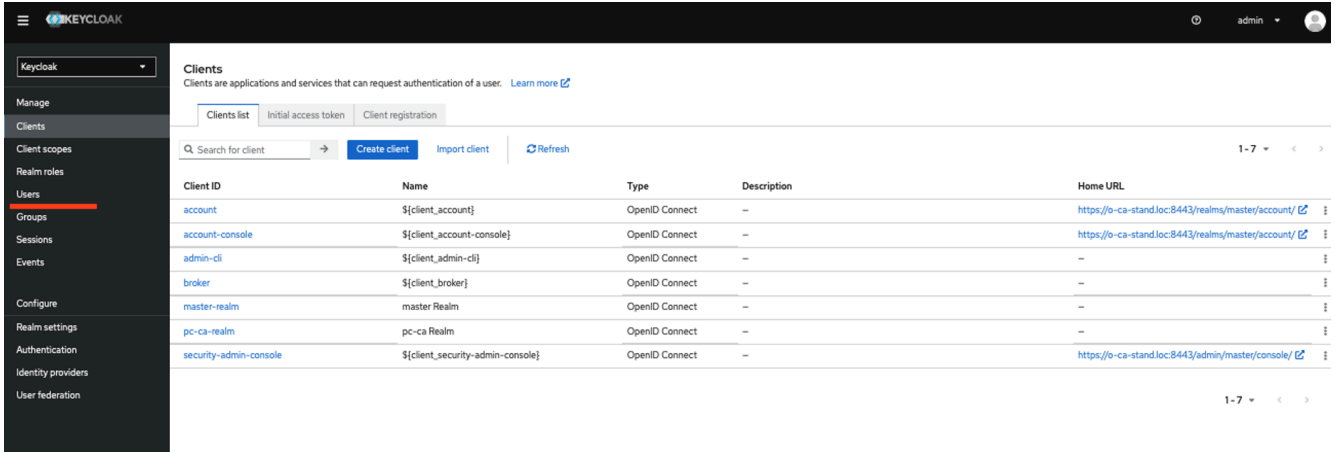
1.1. Создание пользователя с ролью Администратор в Сервисе управления доступом (KeyCloak)

Перед входом в авторизованную зону web-интерфейса ST CA необходимо добавление пользователя KeyCloak, в случае если не была настроена интеграция с Active Directory или другими системами идентификации и аутентификации.

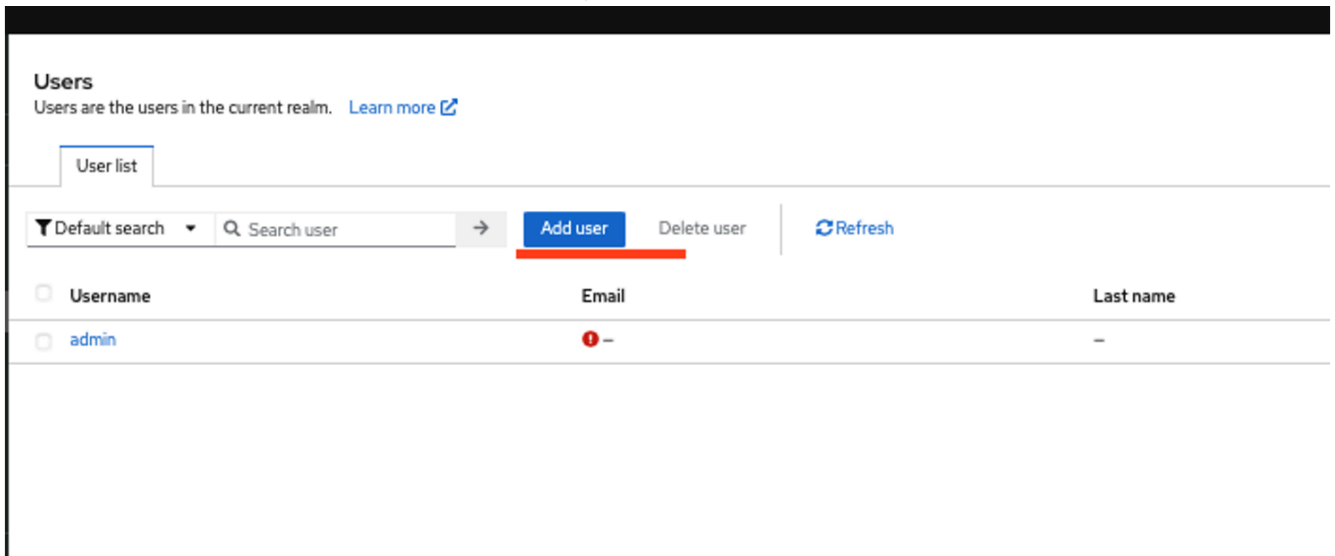
1. Для этого необходимо авторизоваться в KeyCloak



2. Перейти в раздел «Users»



3. Создать нового пользователя, нажав кнопку «Add user»



4. Заполнить форму данными пользователя

Create user

Required user actions

Email verified No

General

Username *

Email

First name

Last name

Groups

Jump to section

[General](#)

- ▶ «Required user actions» – (опционально) выбор сценария аутентификации пользователя, возможность многофакторной аутентификации для пользователя.
- ▶ «Email verified» – (опционально) требуется ли подтверждение электронной почты перед авторизацией.
- ▶ «Username» – уникальное имя пользователя.
- ▶ «Email» – (опционально) адрес электронной почты пользователя.
- ▶ «First name» – Имя пользователя.
- ▶ «Last name» – Фамилия пользователя.
- ▶ «Groups» – (опционально) определения пользователя в конкретную группу, если они были заведены ранее.

Для создания пользователя необходимо нажать кнопку «Create».

5. После того, как пользователь будет создан, откроется меню с возможностью настройки прав пользователя

Users > User details

astest Enabled Action

Details | Credentials | Role mapping | Groups | Consents | Identity provider links | Sessions

ID * ddd557b6-1ca2-456e-a268-d085c21c375e

Created at * 6/24/2024, 4:29:33 PM

Required user actions Select action

Email verified No

General Jump to section

Username * astest General

Email

First name anna

Last name senina

Save Revert

- ▶ Details – раздел, позволяющий отредактировать основную информацию о пользователе, задаваемую при регистрации.
- ▶ Credential – раздел, позволяющий задать/восстановить пароль пользователя.

Details | Credentials | Role mapping | Groups | Consents | Identity provider links | Sessions

Type	User label	Created at	Data
Password		3/26/2024, 6:11:46 PM	Show data

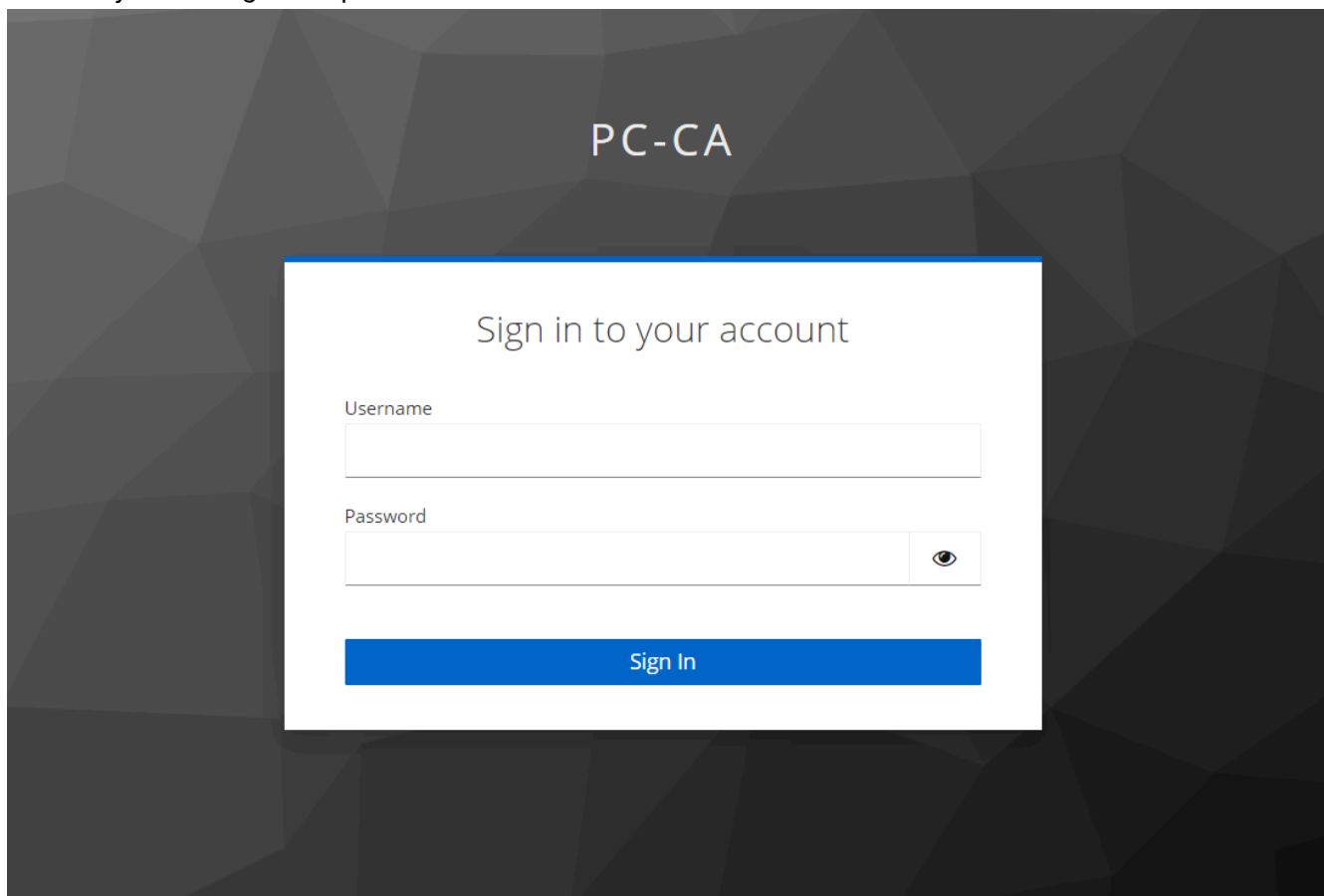
Reset password

- ▶ Role mapping – раздел, позволяющий задать права пользователя. Для добавления роли требуется нажать кнопку «Assign role», затем выбрать доступную роль из списка.

Name	Inherited	Description
default-roles-master	False	`\${role_default-roles}`
admin	False	`\${role_admin}`
pc-ca-realm manage-events	False	`\${role_manage-events}`
pc-ca-realm view-authorization	False	`\${role_view-authorization}`
pc-ca-realm manage-clients	False	`\${role_manage-clients}`
pc-ca-realm view-events	False	`\${role_view-events}`
pc-ca-realm manage-users	False	`\${role_manage-users}`
pc-ca-realm manage-authorization	False	`\${role_manage-authorization}`
pc-ca-realm view-identity-providers	False	`\${role_view-identity-providers}`
pc-ca-realm query-users	False	`\${role_query-users}`

Заполнение остальных разделов производится опционально и зависит от первоначальных настроек стенда.

- После того, как пользователь был создан, он может авторизоваться в web-интерфейсе ST CA, используя свои login и пароль.



1.2. Авторизация в Личном Кабинете Администратора

Для начала работы с Личным кабинетом Пользователю необходимо перейти по адресу личного кабинета в используемом Браузере.

Браузеры, доступные для работы:

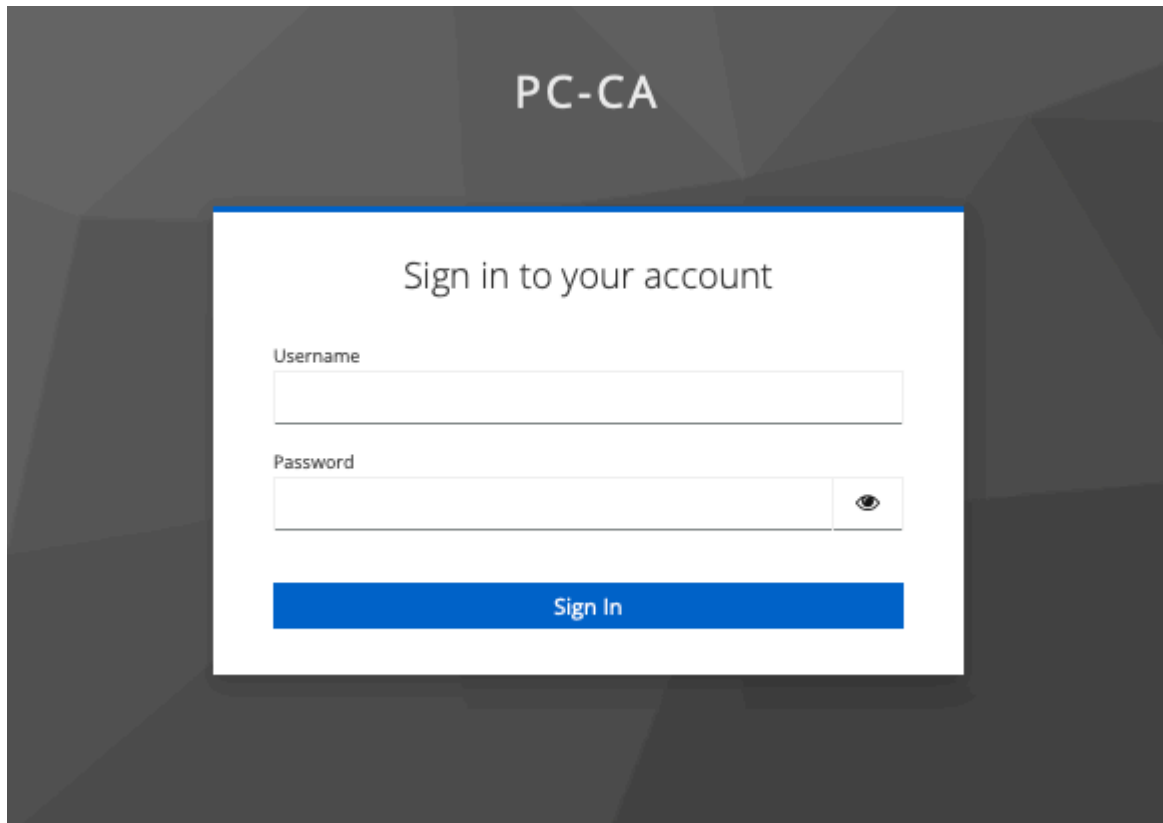
- ▶ Chromium 90 (Chrome, Edge);
- ▶ Firefox 88;
- ▶ Safari 15.

Не поддерживаются браузеры:

- ▶ Edge (версия < 79);

- ▶ Internet Explorer.

В открывшейся форме необходимо указать логин и пароль, выданный пользователю с ролью Администратор.



2. Основной интерфейс

1. Попав в авторизованную зону ST CA, Администратор увидит основные разделы интерфейса.

- ▶ Раздел «ST CA Local Stand» - статистика по выпущенным сертификатам, а также общая информация о центре сертификации. Имя раздела – это имя самого Центра сертификации.

- ▶ Раздел «Сертификаты» - работа с сертификатами, выпущенными на конкретном экземпляре Центра сертификации.
- ▶ Раздел «Запросы» - работа с запросами на выпуск сертификата на конкретном экземпляре Центра сертификации.
- ▶ Раздел «Настройки» - создание и управление шаблонами сертификатов, работа со справочниками Центра сертификации и настройкой правил email-рассылки.

Настройки в свою очередь состоят из трех подразделов:

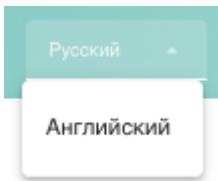
- ▶ Настройка шаблонов Центра Сертификации;
- ▶ Настройка справочников Центра Сертификации;
- ▶ Настройка email-рассылки.

2.1. Глобальные настройки

2.1.1. Переключение языка

В шапке Личного кабинета Администратору доступна функция переключения языка:

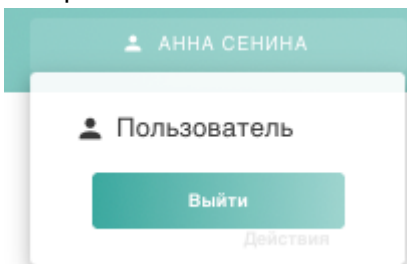
- ▶ русский;
- ▶ английский.



При этом локаль браузера, выбранная Администратором, определяется Личным кабинетом автоматически, что позволяет открывать Личный кабинет в соответствии с выбранной Администратором локалью автоматически.

2.1.2. Выход из Личного кабинета

В шапке Личного кабинета Администратора при нажатии на логин Администратор может выйти из авторизованной зоны.

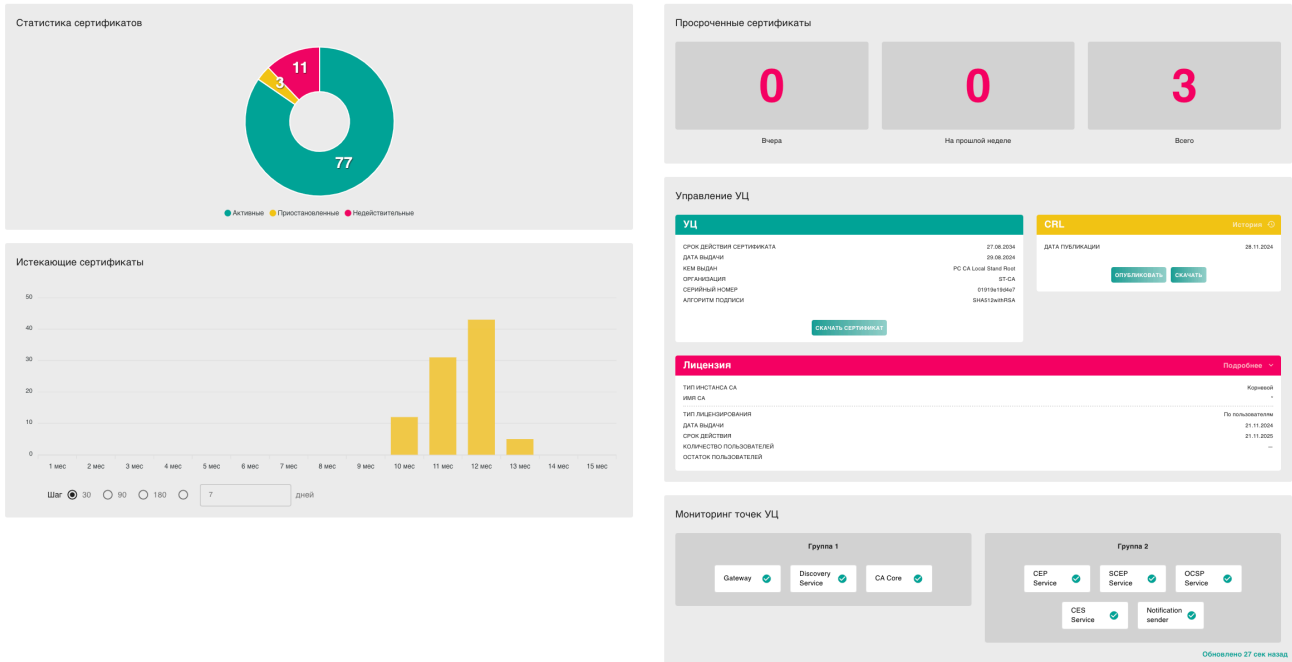


2.1.3. Смена роли

Если учетной записи Администратора присвоено несколько ролей, например, Пользователя и Администратора/Оператора/Аудитора, при нажатии на свой логин в шапке Личного кабинета ему станет доступна кнопка "Сменить роль". Нажав на неё, Администратор сможет ознакомиться со списком доступных ему ролей и переключиться на Личный кабинет другой роли.

3. Раздел «ST CA Local Stand»

ST CA Local Stand



1. Виджет «Статистика сертификатов» - круговая диаграмма, демонстрирующая количество сертификатов в конкретном статусе: активные, приостановленные, недействительные.
2. Виджет «Просроченные сертификаты» - информация о количестве просроченных сертификатов: вчера, на прошлой неделе, за весь период времени.
3. Виджет «Истекающие сертификаты» - гистограмма с количеством истекающих сертификатов через установленный период времени. Администратор может установить удобную периодичность отображения столбцов диаграмм.
4. Виджет «Мониторинг точек УЦ» - отображает информацию о подключении отдельных микросервисов удостоверяющего центра.
5. Виджет «Управление УЦ» - отображает общую информацию об удостоверяющем центре и действующем экземпляре удостоверяющего центра:
 - ▶ раздел УЦ – содержит в себе информацию о корневом сертификате удостоверяющего центра. При нажатии на кнопку «Скачать корневой сертификат» Администратор может скачать сертификат на

свой компьютер. Подробнее об отражаемой в виджете информации в п.2.1.1.

УЦ

СРОК ДЕЙСТВИЯ СЕРТИФИКАТА	27.08.2034
ДАТА ВЫДАЧИ	29.08.2024
КЕМ ВЫДАН	PC CA Local Stand Root
ОРГАНИЗАЦИЯ	ST-CA
СЕРИЙНЫЙ НОМЕР	01919e19d4e7
АЛГОРИТМ ПОДПИСИ	SHA512withRSA

СКАЧАТЬ СЕРТИФИКАТ

- ▶ раздел «CRL» позволяет ознакомиться с датой последней публикации списка отозванных сертификатов (CRL), а также историей публикаций. При нажатии на кнопку «Скачать» начинается скачивание CRL. При нажатии на кнопку «Опубликовать» происходит публикация актуального CRL.
- ▶ Раздел «Лицензия» позволяет ознакомиться с информацией о лицензии продукта SafeTech CA, а именно дате выдачи лицензии и сроке ее действия.

Лицензия
Кратко ^

ТИП ИНСТАНСА СА	Корневой
ИМЯ СА	*
ТИП ЛИЦЕНЗИРОВАНИЯ	
	По пользователям
ДАТА ВЫДАЧИ	21.11.2024
СРОК ДЕЙСТВИЯ	21.11.2025
КОЛИЧЕСТВО ПОЛЬЗОВАТЕЛЕЙ	—
ОСТАТОК ПОЛЬЗОВАТЕЛЕЙ	
ИНТЕРФЕЙС РАБОТЫ С КЛЮЧАМИ	
	cp_jcsp, pkcs11, pkcs12
ДОПОЛНИТЕЛЬНЫЕ МОДУЛИ	ca-ser, ca-ces, ca-scep, ca-acme, ca-ui, ca-ocsp, notification-sender, ca-gateway, crl-dp, aia

3.1. Информация о сертификате Центра сертификации.

В виджете представлена основная информация из сертификата корневого/подчиненного инстанса Центра сертификации.

Таблица 1. Состав информации сертификата об инстансе Центра сертификации.

№	Поле виджета	Описание
1	Срок действия сертификата	Дата истечения сертификата инстанса Центра сертификации
2	Дата выдачи	Дата выпуска сертификата инстанса Центра сертификации
3	Кем выдан	Центр сертификации, выпустивший сертификат для инстанса Центра сертификации
4	Организация	Наименование организации-владельца инстанса Центра сертификации
5	Серийный номер	Серийный номер сертификата инстанса Центра сертификации
6	Алгоритм подписи	Алгоритм подписи инстанса Центра сертификации

3.2. Информация о лицензии Центра сертификации.

В виджете представлена информация о лицензии, установленную на инстансе Центра сертификации.

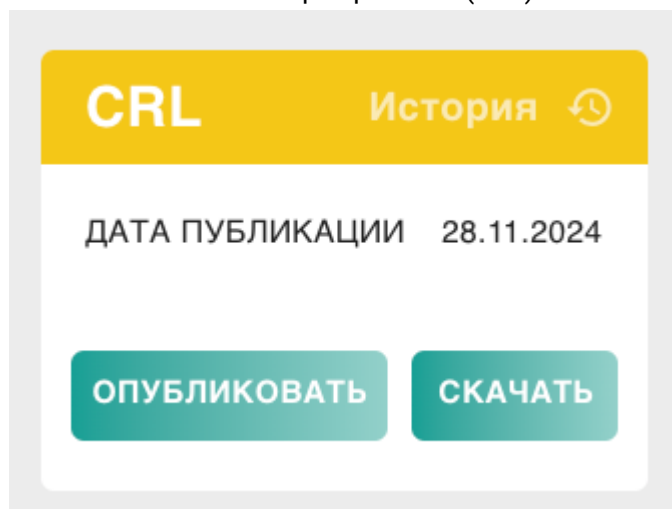
Таблица 2. Состав информации о лицензии Центра сертификации.

№	Поле виджета	Описание
1	Тип инстанса	Тип инстанса Центра сертификации: корневой или подчиненный.
2	Имя CA	DN инстанса Центра сертификации
3	Тип лицензирования	Способ лицензирования инстанса Центра Сертификации: по пользователям или по сертификатам
4	Дата выдачи	Дата выдачи Лицензии
5	Срок действия	Дата, когда срок действия Лицензии закончится
6	Количество пользователей/сертификатов	Общее количество на инстансе пользователей/сертификатов, предусмотренных лицензией

7	Остаток пользователей/ сертификатов	Остаток доступных на инстансе пользователей/ сертификатов, предусмотренных лицензией
8	Интерфейс работы с ключами	Предусмотренные лицензией доступные интерфейсы работы с ключами: КриптоПро HSM, PKCS#11, PKCS#12
9	Дополнительные модули	Набор доступных по лицензии дополнительных функциональных модулей Центра сертификации











3.3. Управление CRL

В виджете управления CRL Администратор может ознакомиться с последней датой публикации списка отозванных сертификатов (CRL).



При нажатии на кнопку "Опубликовать" формируется обновленный CRL, после чего происходит его публикация. При нажатии на кнопку "Скачать" начнется скачивание последнего опубликованного CRL.

История выпущенных CRL

id	Дата публикации	Скачать
1	11.09.2024 10:18:43	
2	11.09.2024 12:00:00	
3	12.09.2024 00:00:00	
4	12.09.2024 12:00:00	
5	13.09.2024 00:00:01	
6	13.09.2024 12:00:00	
7	14.09.2024 00:00:00	
8	14.09.2024 12:00:00	
9	15.09.2024 00:00:00	
10	15.09.2024 12:00:00	

Элементов на странице:

10



1 — 10 из 162



Закреть

При нажатии на кнопку История Администратор сможет ознакомиться со всей историей опубликованных ранее CRL и скачать их.

4 Раздел «Сертификаты»

Сертификаты

Действия: [+ ДОБАВИТЬ](#) [↑ ЗАГРУЗИТЬ](#) [✓ СОЗДАТЬ](#) [✚ ИМПОРТИРОВАТЬ СЕРТИФИКАТЫ](#) С выбранными: [|| ПРИОСТАНОВИТЬ](#) [▶ ВОЗОБНОВИТЬ](#) [> ОТОЗВАТЬ](#) [⚡ СКАЧАТЬ](#) [📄 СФОРМИРОВАТЬ В ФОРМАТЕ EXCEL](#)

<input type="checkbox"/>	Дата выпуска ↓	Дата истечения	Серийный номер	Шаблон	CN	O	OU	E	Статус	Действия	⚙
<input type="checkbox"/>	25.11.2024	25.11.2025	68	User_ST_CA	анна сенина			a.senina@safe-tech.ru	🟢	🔄 🛑 📄	
<input type="checkbox"/>	25.11.2024	25.11.2025	65	User_ST_CA_auto	анна сенина			a.senina@safe-tech.ru	🟢	🔄 🛑 📄	
<input type="checkbox"/>	25.11.2024	25.11.2025	64	User_ST_CA	Анна			a.senina@safe-tech.ru	🟢	🔄 🛑 📄	
<input type="checkbox"/>	25.11.2024	25.11.2025	62	MS_ENROLLMENT_COMP_AUTO	o-ca-stand-dc.domain.o-ca-stand.loc				🟢	🔄 🛑 📄	
<input type="checkbox"/>	25.11.2024	25.11.2025	61	User_ST_CA	Сенина Анна Сергеевна	SafeTech Ltd.	Dev	asenina@safe-tech.local	🟢	🔄 🛑 📄	
<input type="checkbox"/>	22.11.2024	22.11.2025	60	MS_ENROLLMENT_COMP_AUTO	o-ca-stand-dc.domain.o-ca-stand.loc				🟢	🔄 🛑 📄	
<input type="checkbox"/>	22.11.2024	22.11.2025	5f	User_ST_CA	анна сенина			a.senina@safe-tech.ru	🟢	🔄 🛑 📄	
<input type="checkbox"/>	22.11.2024	22.11.2025	5d	User_ST_CA	Сенина Анна Сергеевна	SafeTech Ltd.	Dev	asenina@safe-tech.local	🟢	🔄 🛑 📄	
<input type="checkbox"/>	22.11.2024	22.11.2025	5c	Web server_ST_CA	debian-ca-test.safe-tech.ru	SafeTech Ltd.	IT		🟢	🔄 🛑 📄	
<input type="checkbox"/>	21.11.2024	21.11.2025	5b	User_ST_CA	анна сенина			a.senina@safe-tech.ru	🟢	🔄 🛑 📄	

Элементов на странице: 10 1 — 10 из 91

Данный раздел позволяет ознакомиться со всеми выпущенными центром сертификации.

4.1. Столбцы таблицы сертификатов Центра Сертификации

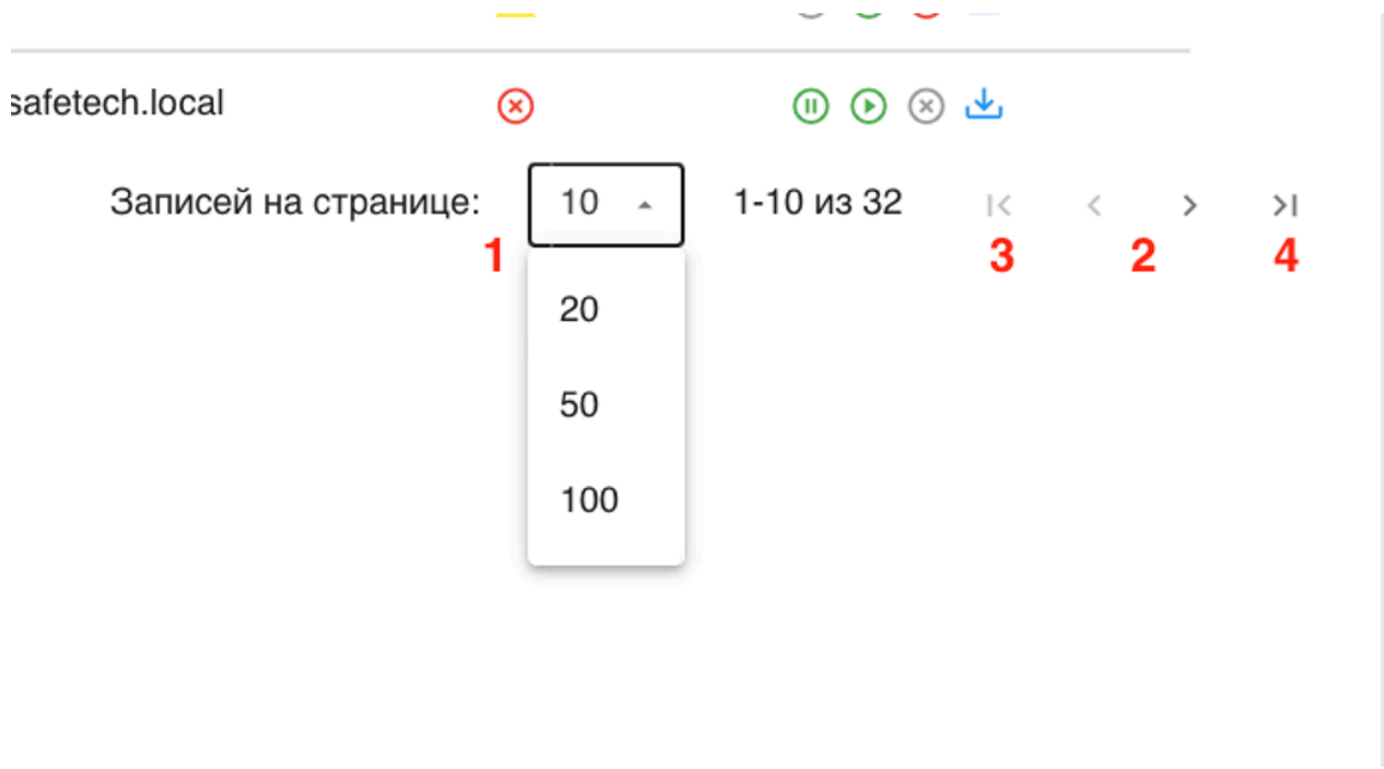
В информационную таблицу о сертификатах Пользователя вынесена основная содержательная информация, которая может потребоваться для поиска и оперативного отслеживания статуса по конкретному сертификату.

Таблица 3. Значения столбцов таблицы сертификатов Центра Сертификации

№	Название столбца	Значение
1	Дата выпуска	Дата выпуска сертификата
2	Дата истечения	Дата истечения срока действия запроса

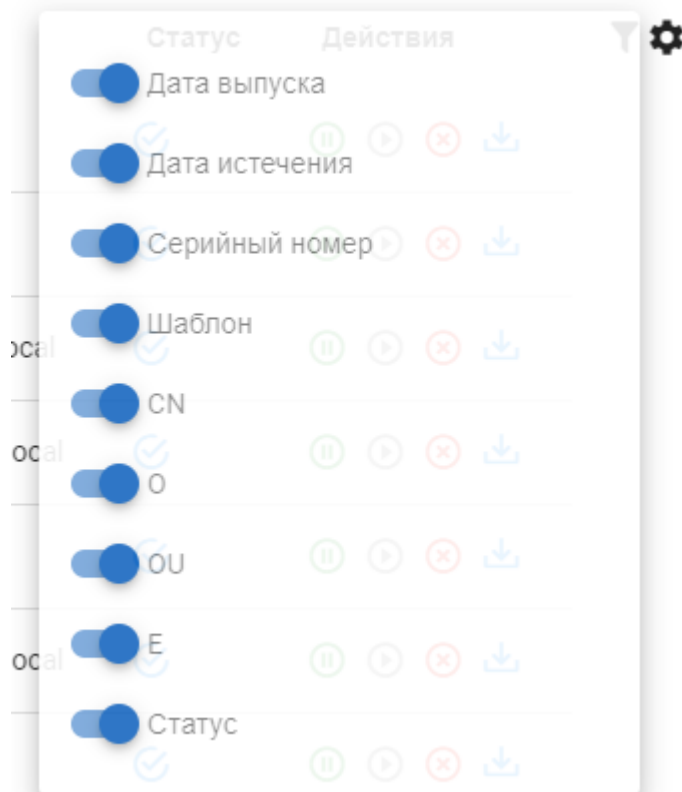
3	CN	Common Name, указанный в сертификате
4	O	Наименование организации, указанное в сертификате
5	OU	Наименование организационного подразделения компании, указанное в сертификате
6	E	Адрес электронной почты, указанный в сертификате
7	Статус	<p>Статус, в котором находится сертификат:</p> <ul style="list-style-type: none">- Активен - сертификат действителен;- Приостановлен - сертификат был приостановлен Пользователем или Администратором;- Просрочен - срок действия сертификата истек;- Отзыван - сертификат находится в списке отзыванных сертификатов и более не действителен.
8	Действия	<p>Действия, доступные пользователю:</p> <ul style="list-style-type: none">- приостановить сертификат;- возобновить сертификат;- отозвать сертификат;- скачать сертификат.

4.2. Сортировка и фильтрация списка сертификатов



Администратор может выбрать удобное для него количество отображаемых записей на странице в правом нижнем углу таблицы (цифра 1). Также Администратор может переключаться между страницами, нажимая на стрелки (цифра 2), а также сразу подключиться на первую или последнюю страницу с помощью крайних стрелок (цифры 3 и 4).

При этом каждый Администратор может настроить отображаемые поля таблицы под себя. Для этого необходимо нажать на «шестеренку» в правом верхнем углу таблицы и выбрать у соответствующего поля необходимый свичер активировать/деактивировать его.



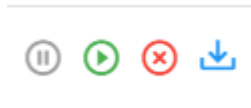
Интерфейс позволяет реализовать поиск сертификатов по полям сертификата. Для поиска необходимо нажать на значок фильтра, после чего откроется дорожка с полями для заполнения.

<input type="checkbox"/>	Дата выпуска ↓	Дата истечения	CN	O	OU	E	Статус	Действия	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

Для осуществления поиска сертификатов возможно задавать одновременно несколько параметров. Для поиска сертификата по статусу необходимо в дорожке поиска оставить набор активных статусов, для активации/деактивации статуса необходимо нажать на него. ![16.png](/ca_admin_guide/16.png)

4.3. Действия с одним сертификатом

Администратор может совершать действия с выбранным сертификатом в таблице, нажав соответствующую кнопку в столбце действий на дорожке выбранного сертификата:




- ▶ Кнопка «пауза» - приостанавливает выбранный сертификат;
- ▶ Кнопка «продолжение» - возобновляет действие выбранного сертификата, который ранее был приостановлен;
- ▶ Кнопка «крестик» - отзывает выпущенный сертификат;
- ▶ Кнопка «скачать» - позволяет начать загрузку выбранного сертификата на устройство.

4.4. Массовые действия с группой сертификатов

Также Администратор может совершать действия одновременно с множеством сертификатов. Для этого Администратор должен выбрать группу сертификатов, с которыми необходимо совершить действия, проставив галочки перед выбранными сертификатами в таблице.

<input type="checkbox"/>	Дата выпуска	Дата истечения	Серийный номер	Шаблон	CN
<input checked="" type="checkbox"/>	14.05.2024	16.09.2024	018f7913bcdb	User	Галкин Евгений Дмитриевич
<input checked="" type="checkbox"/>	22.05.2024	24.09.2024	018fa03c4e90	User	Галкин Евгений Дмитриевич
<input checked="" type="checkbox"/>	12.04.2024	06.07.2025	018ed24d9998	User	egalkin
<input type="checkbox"/>	12.04.2024	12.04.2025	018ed2a6c1e6	User	Evgenii Galkin

Для сброса выбранной группы сертификатов необходимо нажать на кнопку «минус» в шапке таблицы сертификатов.

	Дата выпуска
<input checked="" type="checkbox"/>	14.05.2024
<input checked="" type="checkbox"/>	22.05.2024
<input checked="" type="checkbox"/>	12.04.2024

После того, как группа сертификатов выбрана, пользователь может выбрать действие, которое требуется совершить с группой сертификатов.

С выбранными

|| ПРИОСТАНОВИТЬ

▶ ВОЗОБНОВИТЬ

× ОТОЗВАТЬ

↓ СКАЧАТЬ

Доступные действия:

1. "Приостановить" - приостановить действие выбранной группы сертификатов, их статус изменится на "Приостановлен";
2. "Возобновить" - возобновить действие выбранной группы сертификатов, все сертификаты должны находиться в статусе "Приостановлен", для них статус изменится на "Активен";
3. "Отозвать" - выбранная группа сертификатов будет не действительна, статус изменится на "Отозван", возобновить действие данных сертификатов больше не будет возможным;
4. "Скачать" - начнется скачивание архива с выбранной группой сертификатов.

4.5. Выпуск сертификата

В разделе сертификатов Администратору доступно три возможных способа выпуска сертификата с помощью кнопок:

1. "Добавить запрос" - загрузка запроса текстом в формате PKCS#10 (кодировка pem).
2. "Загрузить запрос" - загрузка файловых запросов.
3. "Создать запрос" - создание запроса на выпуск сертификата из web-интерфейса Личного кабинета Пользователя.

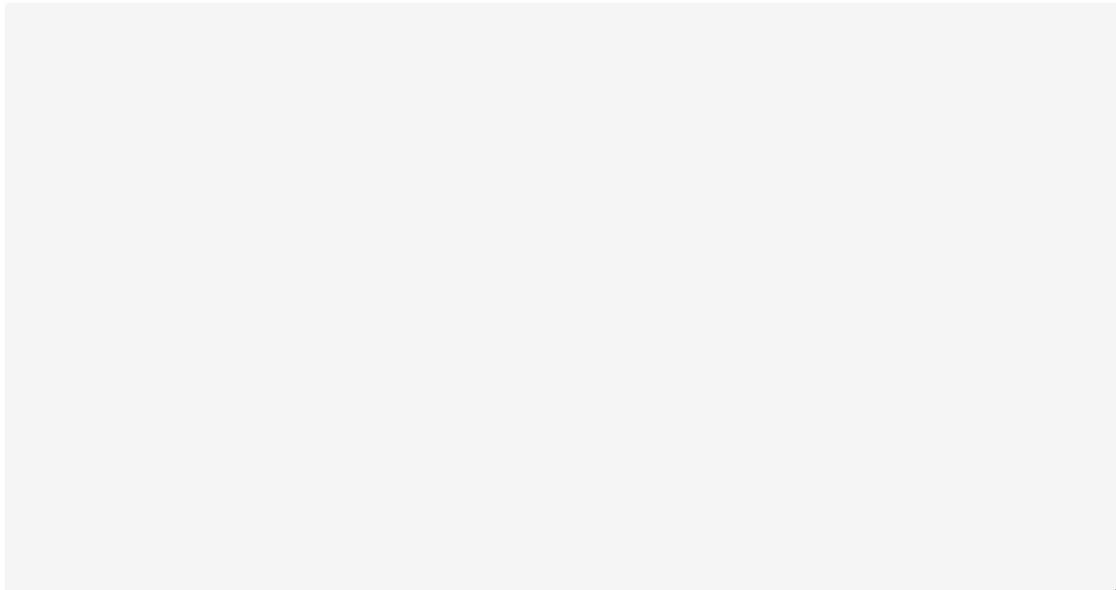
4.5.1. Текстовый запрос на выпуск сертификата

Для подгрузки текстового запроса Администратору необходимо:

1. нажать на кнопку "добавить" в разделе "Действия", после чего требуется загрузить текст запроса в формате PKCS#10 (кодировка pem) в поле открывшегося окна.

🔑 ЗАПОЛНИТЕ ЗАПРОС НА ВЫПУСК СЕРТИФИКАТА

Укажите данные запроса в формате PKCS#10 *



Запрос должен быть представлен в кодировке utf8

ПОСМОТРЕТЬ СОСТАВ ЗАПРОСА

ПОДТВЕРДИТЬ

ОТМЕНИТЬ

2. нажать на кнопку "Подтвердить", после чего сертификат будет выпущен и отразится в таблице сертификатов.

Пользователь может ознакомиться с составом запроса, нажав на кнопку "Посмотреть состав запроса".

4.5.2. Файловый запрос на выпуск сертификата

Для массового выпуска сертификатов Администратор может воспользоваться функциональностью выпуска сертификатов с помощью загрузки файловых запросов. Также Администратор данным способом может выпустить и единственный сертификат. Для этого необходимо:

1. нажать на кнопку "Загрузить запрос", после чего требуется загрузить файлы запросов в открывшееся окно;

ЗАГРУЗИТЕ АРХИВ ИЛИ ФАЙЛЫ С ЗАПРОСАМИ НА ВЫПУСК СЕРТИФИКАТОВ



Максимум 20 файлов. Поддерживаемые расширения: .csr, .req, .pem, .der, .p10, .txt, .zip






ЗАГРУЗИТЬ

ОТМЕНИТЬ

2. нажать на кнопку "Подтвердить", после чего сертификаты будут выпущены и отразятся в таблице сертификатов.

Администратор может загрузить максимально за одну итерацию 20 файлов форматов: csr, req, pem, der, p10, txt, zip. Zip-архив может включать в себя группу запросов на выпуск сертификата.

Администратор может ознакомиться с составом запроса, нажав на кнопку "Документ" рядом с запросом.

 Сенина Анна Сергеевна.p10  

Состав запроса

Уникальное имя (DN)

CN:	Сенина Анна Сергеевна
O:	SafeTech Ltd.
OU:	Dev
E:	asenina@safetech.local

Информация об открытом ключе

Алгоритм:	RSA
Длина ключа:	2048 bit

Использование ключа

Подпись

Шаблон

User ST_CA

Расширения использования ключей (EKU)

1.3.6.1.5.5.7.3.2 (Client Authentication)

При отсутствии информации о шаблоне в запросе Администратор может его выбрать в разделе предпросмотра состава запроса.

4.5.3. Создание запроса на выпуск сертификата из формы

Администратор может сформировать запрос прямо из Личного кабинета (данная функциональность доступна только при работе с шаблонами протокола ST-CA). Для этого Администратору необходимо:

1. нажать на кнопку "Создать запрос", после чего станет доступна форма создания запроса на выпуск сертификата;

🔗 Создание запроса

Выберите шаблон ▼

* Обязательное поле

1. Выберите алгоритмы для формирования запроса на выпуск сертификата*

Выберите алгоритм для ключей

RSA ECDSA EDDSA GOST

Выберите алгоритм подписи ▼

* Обязательное поле

Длина ключа*

Выберите длину ключа ▼

* Обязательное поле

! Минимальная длина ключа, установленная шаблоном

2. Заполните Subject и SAN*

Компоненты Subject ^

Название компонента	Значение	Действия
Выберите название компонента ▼	Введите значение	+
CN	анна сенина	🗑️
DC	Выберите один из вариантов ▼ <small>* Обязательное поле</small>	🗑️
E	a.senina@safe-tech.ru	🗑️

2. выбрать шаблон из списка доступных;

3. Администратору необходимо выбрать алгоритм для формирования запроса.

При выборе алгоритма для ключей RSA Администратору будут доступны алгоритмы подписи SHA256withRSA, SHA384withRSA, SHA512withRSA. В зависимости от выбранного алгоритма для Администратора будут меняться доступные длины ключа:

- ▶ "SHA512withRSA" - 1024 бита, 2048 бит, 4096 бит
- ▶ "SHA384withRSA" - 1024 бита, 2048 бит, 4096 бит
- ▶ "SHA256withRSA" - 512 бит, 1024 бита, 2048 бит, 4096 бит

При выборе алгоритма для ключей ECDSA Администратору будут доступны алгоритмы подписи SHA256withECDSA, SHA384withECDSA, SHA512withECDSA. Администратору потребуется выбрать KeySpec: (prime256v1, secp384r1, secp521r1).

При выборе алгоритма для ключей EDDSA Администратору останется указать только алгоритм подписи Ed25519.

При выборе алгоритма для ключей GOST Администратору потребуются сделать выбор между алгоритмами подписи:

- GOST3411_2012_256withGOST3410_2012_256
- GOST3411_2012_512withGOST3410_2012_512

4. Администратору необходимо заполнить компоненты Subject и SAN

При заполнении компонентов Subject часть данных будет подтянута автоматически из Сервиса управления доступом в случае, если Администратор укажет необходимого пользователя.

2. Заполните Subject и SAN*

Компоненты Subject		
Название компонента	Значение	Действия
Выберите название компонента	Введите значение	+
CN	анна сенина	🗑
DC	Выберите один из вариантов * Обязательное поле	🗑
E	a.senina@safe-tech.ru	🗑

Если данных будет недостаточно или Администратор не укажет пользователя для автоматического заполнения компонент, Администратор может самостоятельно добавить компоненты в первой строке таблицы из доступного ему списка и указать необходимые значения. Для добавления компонента в список, Администратору необходимо нажать "плюс".

Администратор может удалить значения, в которых нет необходимости для формирования запроса на выпуск сертификата, нажатием кнопки "корзина" в действиях.

При заполнении компонентов SAN часть данных будет подтянута автоматически из Сервиса управления доступом.

Компоненты SAN		
Название компонента	Значение	Действия
Выберите название компонента ▾	Введите значение	+
dn	CN=Анна Сенина,CN=Users,DC=domain,DC=o-ca-stand,DC=loc	🗑
upn	a.senina@domain.o-ca-stand.loc	🗑
guid	8i+uOZQYSU6yx5jodML4rg==	🗑
email	a.senina@safe.tech.ru	🗑

Если данных будет недостаточно или Администратор не укажет пользователя для автоматического заполнения компонент, он может самостоятельно добавить компоненты в первой строке таблицы из доступного ему списка и указать необходимые значения. Для добавления компонента в список, Администратору необходимо нажать "плюс".

Администратор может удалить значения, в которых нет необходимости для формирования запроса на выпуск сертификата, нажатием кнопки "корзина" в действиях.

В случае если в выбранном шаблоне были указаны обязательные для заполнения компоненты, они будут подсвечены как обязательные для заполнения.

5. Администратору необходимо задать пароль от PFX контейнера, который будет сформирован при создании запроса на выпуск сертификата.

3. Задайте пароль для PFX контейнера*

Автоматически сгенерировать пароль

Пароль не более 20 символов 0 / 20

Администратор может задать пароль самостоятельно, количество символов пароля не должно превышать 20. Также Администратор может выбрать опцию автоматической генерации пароля, в этом случае пароль будет передан Администратору вместе с PFX-контейнером.

6. дополнительно Администратор может ознакомиться с настройками шаблона, такими как:

- ▶ срок действия сертификата;
- ▶ политики использования ключей, предусмотренные шаблоном;
- ▶ расширения использования ключей (EKU);
- ▶ атрибуты запроса на сертификат.

7. нажать на кнопку "Подтвердить", после чего сертификат будет выпущен и отобразится в таблице сертификатов.

4.6. Выгрузка статистики о сертификатах

Администратор для отчетности или работы со статистикой может настроить фильтрацию необходимых для него сертификатов и нажать кнопку "Сформировать в формате Excel".



Когда таблица в формате Excel будет сформирована, станет активной кнопка "Скачать Excel".



В самой таблице будет приведена вся сводная информация о сертификатах, в соответствии с установленной на таблице сертификатов фильтрацией.

серийный номер	дата выпуска	дата истечения	статус	CN	O	OU	E	шаблон
4b	2024-11-19 11:00:16	2025-11-19 11:00:16	REVOKED	Сенина Анна Сергеевна	SafeTech Ltd.	Dev		User ST_CA
2e	2024-10-30 14:28:25	2025-10-30 14:28:25	SUSPENDED	o-ca-stand-dc.domain.o-ca-stand.loc				MS_ENROLLMENT_COMP_AUTO
2d	2024-10-21 12:27:37	2025-10-21 12:27:37	SUSPENDED	o-ca-stand-dc.domain.o-ca-stand.loc				MS_ENROLLMENT_COMP_AUTO
2c	2024-10-21 12:26:46	2025-10-21 12:26:46	SUSPENDED	Administrator				MS_ENROLLMENT_USER_AUTO
26	2024-10-15 11:55:23	2025-10-15 11:55:23	REVOKED	o-ca-stand-dc.domain.o-ca-stand.loc				MS_ENROLLMENT_COMP_AUTO
25	2024-10-15 11:44:01	2025-10-15 11:44:01	REVOKED	Галкин Евгений Дмитриевич	SafeTech Ltd.	Dev		User ST_CA
24	2024-10-15 11:37:12	2025-10-15 11:37:12	REVOKED	Галкин Евгений Дмитриевич	SafeTech Ltd.	Dev		User ST_CA
23	2024-10-15 09:37:37	2025-10-15 09:37:37	REVOKED	Галкин Евгений Дмитриевич	SafeTech Ltd.	Dev		User ST_CA
1f	2024-10-10 09:15:44	2025-10-10 09:15:44	REVOKED	Сенина Анна Сергеевна	SafeTech Ltd.	Dev		User ST_CA
1d	2024-10-01 12:16:24	2025-10-01 12:16:24	REVOKED	Сенина Анна Сергеевна	SafeTech Ltd.	Dev		User ST_CA
10	2024-09-24 13:41:25	2025-09-24 13:41:25	REVOKED	o-ca-stand-dc.domain.o-ca-stand.loc				MS_ENROLLMENT_COMP_AUTO
0d	2024-09-24 12:02:03	2025-09-24 12:02:03	REVOKED	Server1				Web server for MS_ENROLLMENT
0a	2024-09-24 11:07:46	2025-09-24 11:07:46	REVOKED	Сенина Анна Сергеевна	SafeTech Ltd.	Dev		User ST_CA
05	2024-09-12 11:09:46	2025-09-12 11:09:46	REVOKED	Сенина Анна Сергеевна	SafeTech Ltd.	Dev		User ST_CA

5. Раздел Запросы Центра Сертификации

В данном разделе Администратор может ознакомиться со всеми запросами на выпуск сертификата данного Центра Сертификации.

🔍 Запросы + ДОБАВИТЬ ЗАПРОС ↑ ЗАГРУЗИТЬ ЗАПРОС ✍ СОЗДАТЬ ЗАПРОС

Дата создания	Дата обновления ↓	CN	Эмитент	Id сертификата	Шаблон	Статус	Причина	Утверждающий	Действия
25.11.2024	25.11.2024	анна сенина	анна сенина		User ST_CA	❌ Отклонён	No reason	administrator	👁
25.11.2024	25.11.2024	анна сенина	анна сенина		User ST_CA	🕒 В ожидании одобрения			👁
25.11.2024	25.11.2024	анна сенина	анна сенина	65	User ST_CA_auto	🚀 Выпущен автоматически			👁
25.11.2024	25.11.2024	Anna	анна сенина	64	User ST_CA	✅ Одобрен		administrator	👁
22.11.2024	22.11.2024	анна сенина	анна сенина	5f	User ST_CA	✅ Одобрен		administrator	👁
21.11.2024	21.11.2024	анна сенина	анна сенина	5b	User ST_CA	✅ Одобрен		administrator	👁

Items per page: 1-6 of 6 ⏪ ⏩

Нажатием кнопки "Создать" Администратор сможет создать запрос на выпуск сертификата из Личного кабинета (подробнее см. п. 4.5.3.).

В таблице отображения запросов предусмотрена пагинация. В связи с чем Администратор может выбрать удобное для себя количество отображаемых в таблице строк.



Администратор может управлять переходом между страницами таблицы с запросами с помощью стрелок в нижнем правом углу таблицы.

Администратор может обновить данные таблицы нажатием на кнопку "Обновление" справа от таблицы.

5.1. Столбцы таблицы запросов Центра сертификации

В информационную таблицу о запросах Центра Сертификации вынесена основная содержательная информация, которая может потребоваться для поиска и оперативного отслеживания статуса по конкретному запросу для выпуска сертификата.

Таблица 4. Значения столбцов таблицы запросов Центра Сертификации

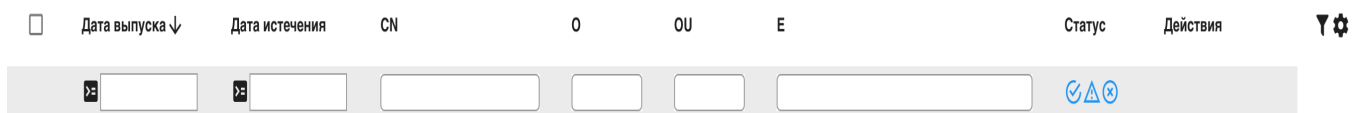
№	Название столбца	Значение
1	Дата создания	Дата направления запроса на выпуск сертификата
2	Дата обновления	Дата изменения статуса запроса
3	CN	Common Name, указанный в запросе на выпуск сертификата
4	Эмитент	Имя Пользователя, отправившего запрос на выпуск сертификата
5	ID сертификата	Серийный номер сертификата, выпущенного по данному запросу. Не указывается в таблице, в случае если запрос на выпуск сертификата был отклонен Администратором
6	Шаблон	Имя шаблона, который указан в запросе на выпуск сертификата
7	Статус	Статус, в котором находится запрос на выпуск сертификата: <ul style="list-style-type: none"> - Выпущен автоматически - сертификат был выпущен по запросу без одобрения Администратора; - Отклонен - запрос на выпуск сертификата был отклонен Администратором; - В ожидании одобрения - запрос ожидает рассмотрения и одобрения Администратора; - Одобрен - запрос на выпуск сертификата был одобрен Администратором и сертификат был выпущен.

8	Причина	Причина отклонения запроса на выпуск сертификата Администратором. В случае одобрения запроса Администратором, значение в столбце не указывается
9	Утверждающий	Имя учетной записи Администратора, принявшего решение об одобрении/отклонении запроса на выпуск сертификата
10	Действия	<p>Действия, доступные пользователю:</p> <ul style="list-style-type: none"> - Предпросмотр состава запроса; - Одобрить запрос (в случае если требуется действие от Администратора); - Отклонить запрос (в случае если требуется действие от Администратора); - Скачать файл запроса.

5.2. Сортировка и фильтрация запросов на выпуск сертификата

Администратор может изменить сортировку списка запросов по каждому из столбцов таблицы от меньшего значения к большему и наоборот. Для сортировки необходимо нажать на название необходимого столбца.

При нажатии на кнопку "Фильтр", справа от таблицы, для Администратора станут доступны поисковые строки по каждому из столбцов таблицы.



При введении Администратором нескольких фильтров одновременно строки в таблице будут отфильтрованы с учетом этих фильтров (логическое "И").

5.3. Действия с запросами Центра Сертификации

Администратору доступно несколько основных действий с запросами на выпуск сертификата:

1. предпросмотр состава запроса - Администратор может ознакомиться с составом запроса в открывшемся модальном окне;
2. одобрение запроса для выпуска сертификата - Администратор может одобрить выпуск сертификату по полученному запросу на выпуск сертификата;
3. отклонение запроса на выпуск сертификата - Администратор может отклонить выпуск сертификата. Дополнительно при отклонении Администратор может указать причину отклонения запроса - она будет доступна Пользователю, направившему запроса в разделе "Запросы Пользователя" в его Личном кабинете;
4. скачать файл запроса.

Действия



5.4. Массовое одобрение/отклонение запросов Администратором

В случае если Администратору необходимо одобрить и отклонить группу запросов, ему необходимо:

1. проставить галки перед запросами, которые требуют совершения действия от Администратора;
2. после выбора запросов станут активными кнопки с выбранными запросами, Администратору необходимо:
 - ▶ нажать кнопку "Одобрить" для выпуска сертификатов по выбранным запросам;
 - ▶ нажать кнопку "Отклонить" для запрета выпуска сертификатов по выбранным запросам.
3. в случае отклонения запросов, Администратору потребуется указать причину отклонения запросов.

6. Раздел «Настройки»

6.1. Настройка Шаблонов Центра Сертификации

[Настройки](#) - [Шаблоны](#)[Создать](#)[Импортировать шаблоны](#)

Наименование шаблона сертификата

MS_ENROLLMENT_COMP_AUTO_dns_dn_full

User_CA_test

User_MS_Enrollment

Web server for MS_ENROLLMENT

MS_ENROLLMENT_COMP_AUTO

MS_ENROLLMENT_COMP_AUTO_dns_dn

SCEP-Default

MS_ENROLLMENT_COMP_AUTO_only_dns

Web server ST_CA

User ST_CA_auto

Элементов на странице:

1 — 10 из 13

|<

<

>

>|

Данный раздел позволяет Администратору создать новый шаблон для выпуска сертификатов или отредактировать ACL уже существующего шаблона.

Для поиска нужного шаблона Администратор может воспользоваться поисковой строкой, начиная вводить искомое название шаблона.

Администратор может посмотреть настройки существующего шаблона, нажав на наименование шаблона в таблице.

Поля шаблона

Наименование
User ST_CA_auto

Тип протокола
ST_CA

Описание
This template is used to issue certificates for users. Digital signature only

Максимальный срок действия сертификата в днях
365

Минимальная длина ключа
2048

Использование ключа

Подпись

Неотрекаемость от авторства

Шифрование ключей

Шифрование данных

Согласование ключей

Подпись сертификатов ключей подписи

Подпись списков отозванных сертификатов

Зашифровывание

Расшифровывание

Всегда проверять уникальность публичного ключа

Обязательные имена субъекта

Роли шаблона

Роли \ Разрешения	Чтение	Чтение/Запись	Выпуск сертификата	Автовыпуск сертификата	Действия
Аудитор	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Внешний	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Оператор	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Пользователь	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Администратор	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Атрибуты сертификата

Название атрибута	Значение атрибута	Критичный
Key Usage	AwHqA==	
Enhanced Key Usage	<автоматически>	
Certificate Template Name	Hh4AVQBzAGUAcgAgAFMAVABI/EMAQQBI/AGEAdQB0AG8=	

Расширения использования ключей (EKU)

Название EKU	Оid
Client Authentication	1.3.6.1.5.5.7.3.2

Сохранить изменения

Удалить шаблон

Создать на основе новый шаблон

6.1.1. Настройка Шаблонов Центра Сертификации

Для создания нового шаблона Администратор может нажать кнопку «Создать», после чего откроется область для задания настроек шаблона.

Поля шаблона

Наименование
Новый шаблон от 2024-11-28T18:46:54.30700

Тип протокола ▼

* Обязательное поле

Описание
Новый шаблон

Максимальный срок действия сертификата в днях *

Минимальная длина ключа
1024 ▼

* Обязательное поле

Использование ключа

* Необходимо выбрать минимум один из вариантов

Подпись Неотрекаемость от авторства Шифрование ключей

Шифрование данных Согласование ключей Подпись сертификатов ключей подписи

Подпись списков отозванных сертификатов Зашифровывание Расшифровывание

Всегда проверять уникальность публичного ключа

Обязательные имена субъекта

[+ ДОБАВИТЬ ИМЯ СУБЪЕКТА](#)

Роли шаблона

[+ ДОБАВИТЬ РОЛЬ](#)

Роли \ Разрешения	Чтение	Чтение/Запись	Выпуск сертификата	Автовыпуск сертификата	Действия
Администратор	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Атрибуты сертификата

[+ ДОБАВИТЬ АТРИБУТ](#)

Название атрибута	Значение атрибута	Критичный	Действия
Key Usage	<автоматически>	<input checked="" type="checkbox"/>	
Certificate Template Name	<автоматически>	<input checked="" type="checkbox"/>	

Расширения использования ключей (EKU)

[+ ДОБАВИТЬ РАСШИРЕНИЕ](#)

[Сохранить изменения](#) [Отменить создание нового шаблона](#)

Для создания нового шаблона Администратору необходимо заполнить поля формы:

1. «Наименование». При создании нового шаблона название задается автоматически, но оно доступно к редактированию. Заданное наименование также будет отображаться в основной таблице со всеми созданными шаблонами.
2. «Описание». Общее описание целей использования создаваемого шаблона.
3. «Максимальный срок действия сертификата в днях». Максимально возможный срок действия сертификата, выпускаемого по данному шаблону. Является числовым значением.
4. «Использование ключа». Доступный набор политик использования ключа, для которого выпускается сертификат. Требуется выбрать хотя бы одну политику.

5. «Минимальная длина ключа». Минимальное значение ключа, ниже которого длина ключа не должна опускаться при выпуске сертификата по настраиваемому шаблону.
6. Опционально Администратор может установить флаг проверки уникальности публичного ключа. В этом случае во всех запросах на выпуск сертификата по данному шаблону будет проверяться был ли ранее в Центре Сертификации уже выпущен с сертификат с аналогичным значением публичного ключа.
7. «Тип протокола». Обязательное поле. SafeTech CA поддерживает несколько протоколов по выпуску ключа, а именно: ST CA, MS Enrollment, SCEP. В зависимости от выбранного типа протокола пользователю могут открываться дополнительные настройки. Так, например, при выборе протокола:
 - ST CA – набор настроек шаблона не изменится;
 - SCEP – набор настроек шаблона не изменится;
 - MS Enrollment – появится дополнительный набор настроек «Доступные флаги».
8. «Доступные флаги». Настройки Enrollment протокола. Смотрите подробнее в п. 6.1.2.
9. Опционально Администратор может установить обязательный для сертификатов, выпускаемых по данному шаблону, набор компонентов Subject.

Для добавления компонента Администратору необходимо нажать кнопку "Добавить имя субъекта".



+ ДОБАВИТЬ ИМЯ СУБЪЕКТА

После чего Администратору станет доступно окно с набором компонентов Subject.

🔍 ВЫБЕРИТЕ ОБЯЗАТЕЛЬНЫЕ ИМЕНА СУБЪЕКТА ИЗ СПИСКА

<input type="checkbox"/>	Название имени субъекта	Oid
<input type="checkbox"/>	C	2.5.4.6
<input type="checkbox"/>	O	2.5.4.10
<input type="checkbox"/>	T	2.5.4.12
<input type="checkbox"/>	OU	2.5.4.11
<input type="checkbox"/>	CN	2.5.4.3
<input type="checkbox"/>	L	2.5.4.7
<input type="checkbox"/>	ST	2.5.4.8

ПОДТВЕРДИТЬ

ОТМЕНИТЬ

В случае отсутствия необходимого компонента в открывшемся списке, Администратор может внести новый компонент в разделе "Справочники". Администратору необходимо проставить галочки напротив обязательных для шаблона компонент. Затем нажать кнопку "Подтвердить".

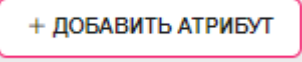
Обязательные имена субъекта
+ ДОБАВИТЬ ИМЯ СУБЪЕКТА

Название имени субъекта	Oid	Действия
C	2.5.4.6	
O	2.5.4.10	
T	2.5.4.12	

Выбранные компоненты будут отображены в настройках шаблона. Администратор может исключить ненужные компоненты из таблицы, нажатием кнопки "Удалить". Или дополнить новыми компонентами, снова нажав кнопку "Добавить имя субъекта".

В случае отсутствия данных компонентов в составе запроса на выпуск сертификата по данному шаблону, пользователю вернется информация о необходимости указать их в запросе. При создании запроса из Личного кабинета данные компоненты будут подсвечены, как обязательные.

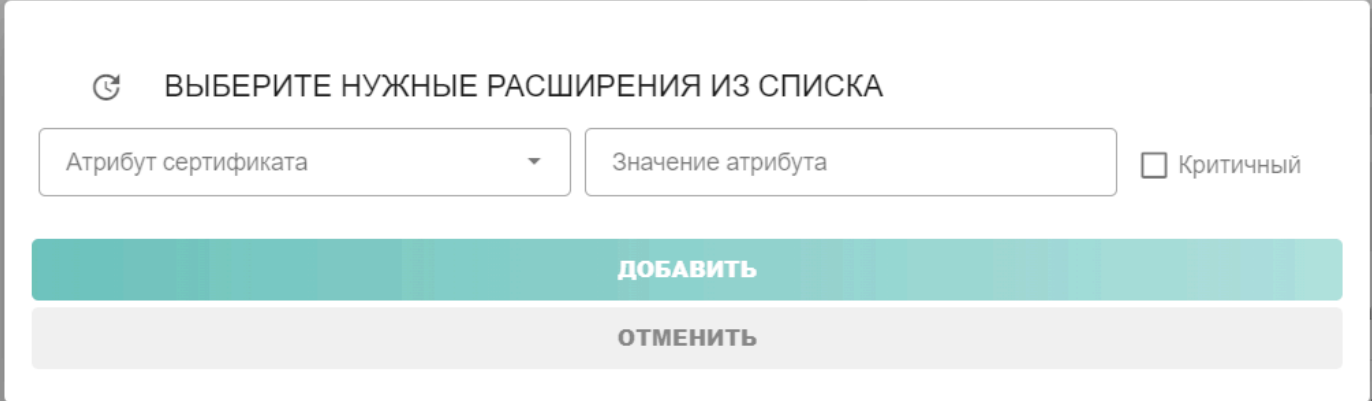
10. «Атрибуты сертификата». Для добавления нового атрибута Администратору необходимо нажать кнопку «+» Добавить атрибут».



После чего Администратор в открывшемся окне выбирает название атрибута сертификата из выпадающего списка. В случае отсутствия требуемого атрибута в списке Администратору необходимо перейти подраздел «Справочники» и добавить необходимый атрибут.

Также Администратор вводит значение атрибута в base64.

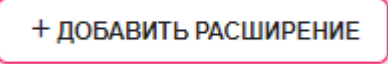
Администратор может задать атрибут в шаблоне сертификата как критичный, для этого он ставит галочку у значения «Критичный». Если его задание опционально, то простановка галочки не требуется.



После того, как поля заполнены, Администратор нажимает кнопку «Добавить». Задаваемый атрибут отразится в таблице атрибутов шаблона сертификатов. В случае если данный атрибут не является для шаблона критичным, Администратор имеет возможность удалить данный атрибут, нажав на кнопку "корзина" в столбце «Действия» напротив него.


Для того чтобы прервать добавления атрибута Администратору необходимо нажать кнопку «Отменить».

11. «Расширения использования ключей (EKU)». Для добавления нового расширения Администратору необходимо нажать кнопку «+ Добавить расширение».



В открывшемся окне Администратору необходимо выбрать требуемые расширения в открывшемся списке, проставив галочку напротив выбранного расширения. Также в данном окне Администратор

может убрать галочку у расширений, которые были выбраны ранее.

 ВЫБЕРИТЕ НУЖНЫЕ РАСШИРЕНИЯ ИЗ СПИСКА

<input type="checkbox"/>	Название расширения	Oid
<input type="checkbox"/>	Microsoft Trust List Signing	1.3.6.1.4.1.311.10.3.1
<input type="checkbox"/>	Encrypting File System	1.3.6.1.4.1.311.10.3.4
<input type="checkbox"/>	Secure Email	1.3.6.1.5.5.7.3.4
<input checked="" type="checkbox"/>	Client Authentication	1.3.6.1.5.5.7.3.2
<input checked="" type="checkbox"/>	Server Authentication	1.3.6.1.5.5.7.3.1
<input type="checkbox"/>	Directory Service Email Replication	1.3.6.1.4.1.311.21.19
<input type="checkbox"/>	Smart Card Logon	1.3.6.1.4.1.311.20.2.2
<input type="checkbox"/>	File Recovery	1.3.6.1.4.1.311.10.3.4.1
<input type="checkbox"/>	KDC Authentication	1.3.6.1.5.2.3.5
<input type="checkbox"/>	Sub CA	1.3.6.1.4.1.32029.1.4.4.3

ПОДТВЕРДИТЬ

ОТМЕНИТЬ

Для добавления в шаблон выбранных расширений, Администратору необходимо нажать кнопку «Подтвердить».

Для того чтобы прервать добавление расширений, Администратору необходимо нажать кнопку «Отменить».

В случае отсутствия требуемого расширения в списке, Администратору необходимо перейти в подраздел «Справочники» и добавить недостающее расширение.

12. «Роли шаблона». Администратор может задать права для каждой предусмотренной роли по действию с данным шаблоном.

Для добавления роли Администратору необходимо нажать кнопку «+ Добавить роль».

+ ДОБАВИТЬ РОЛЬ

После чего Администратору станет доступна строка для выбора роли и настройки прав.

Роли шаблона					
Роли \ Разрешения	Чтение	Чтение/Запись	Выпуск сертификата	Автовыпуск сертификата	Действия
Без роли	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Администратор в выпадающем списке выбирает роль. На данный момент в ST CA предусмотрены следующие роли:

- Администратор;
- Оператор;
- Пользователь;
- Аудитор;
- Внешний.

После чего выбирает соответствующий для роли набор прав, активируя галочки в соответствующих столбцах.

- Право «Чтение» - возможность просмотра данного шаблона.
- Право «Чтение/Запись» - возможность просмотра и редактирования данного шаблона.
- Право «Выпуск сертификата» - возможность выпуска сертификата по данному шаблону.
- Право «Автовыпуск сертификата» - возможность автоматического выпуска сертификата по данному шаблону.

В случае если для роли Пользователь для выбранного шаблона Администратор устанавливает право "Выпуск сертификата", то все запросы на выпуск сертификата Пользователя, будут направлены на одобрение/отклонение Администратору. Если же Администратор устанавливает право "Автовыпуск сертификата", то все сертификаты Пользователя будут выпускаться без одобрения Администратором.

Для удаления настроек роли Администратору необходимо нажать кнопку корзины в строке, соответствующей выбранной роли.

После того, как все настройки заданы, Администратор нажимает кнопку «Сохранить изменения».

Сохранить изменения

Затем возникает дополнительное окно подтверждения:

- Для сохранения созданного шаблона Администратору необходимо нажать кнопку «Сохранить на сервер».
- Для прерывания создания шаблона Администратору необходимо нажать кнопку «Отменить правку».
- Для возвращения к созданию шаблону Администратору необходимо нажать кнопку «Продолжить редактирование».



Подтвердите действие

Сохранить изменения шаблона сертификата?

ПРОДОЛЖИТЬ РЕДАКТИРОВАНИЕ

ОТМЕНИТЬ ПРАВКУ

СОХРАНИТЬ НА СЕРВЕР

Шаблон становится доступным к просмотру в списке шаблонов сертификатов.

6.1.2. Описание настроек раздела «Доступные флаги»

Набор настроек «Доступные флаги» включает в себя несколько параметров:

1. Параметр для определения правил заполнения атрибутов сертификата, связанных с субъектом: Subject, Subject Alternative Name (SAN):
 - ▶ Компоненты субъекта Subject, SAN могут быть указаны в самом запросе – кнопка «Указать в запросе». При таком разрешении дополнительных настроек шаблона не потребуется;
 - ▶ Компоненты субъекта Subject, SAN заполняются из информации в Active Directory (AD) – кнопка «Построить на основе информации Active Directory». Потребуется настроить набор информации, которая будет подтягиваться из AD, а именно, выбрать формат имени субъекта в выпадающем списке.

Доступные флаги

Параметр для определения правил заполнения атрибутов сертификата, связанных с субъектом: Subject, Subject Alternative Name (SAN)

- Указать в запросе Построить на основе этой информации Active Directory

Формат имени субъекта
none

none

DNS как CN

Общее имя

Путь к каталогу

Выбрать разрешение о выключении Адреса электронной почты в имя субъекта.

- Включить адрес электронной почты в имя субъекта

Выбрать набор информации из AD, которая будет входить в SAN.

Включить эту информацию в SAN

- DNS значение корня Имя пользователя (UPN) GUID
 Имя участника службы (SPN) Имя электронной почты DNS-имя

- Параметр для определения дополнительных правил выпуска сертификата на УЦ (значение параметра = 1 и не изменяемо);
- msGeneralFlags – свое значение маски для субъекта – 0;
- Выберите тип субъекта - параметр служит для определения типа конечного субъекта, где пользователь - 0, компьютер - 65).

1
Параметр для определения дополнительных правил выпуска сертификата на УЦ

Тип субъекта
Пользователь

msGeneralFlags
0
Свое значение маски для субъекта

Пользователь
Компьютер

6.1.3. Редактирование существующего шаблона

Администратор может не только создавать новые шаблоны, но и редактировать доступность шаблона различным категориям пользователей.

Примечание: редактирование остальных атрибутов шаблона не доступно после создания шаблона, в случае необходимости изменения остальных атрибутов Администратору необходимо создать копию выбранного шаблона и выполнить обновление атрибутов в ней, исходный шаблон затем допускается удалить.

Для этого ему необходимо выбрать из общего списка шаблонов сертификата необходимый шаблон, нажав на его название. После чего раздел «Роли шаблона» будет доступен к редактированию.

Поля шаблона

Наименование: Тип протокола:

Описание:

Максимальный срок действия сертификата в днях: Минимальная длина ключа:

Использование ключа

Подпись
 Неотрекаемость от авторства
 Шифрование ключей
 Шифрование данных
 Согласование ключей
 Подпись сертификатов ключей подписи
 Подпись списков отзыванных сертификатов
 Зашифровывание
 Расшифровывание

Роли шаблона + добавить роль

Роли \ Разрешения	Чтение	Чтение/Запись	Выпуск сертификата	Автоматический выпуск сертификата	Действия
Администратор	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Аудитор	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Оператор	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Внешний	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Атрибуты сертификата

Название атрибута	Значение атрибута	Критичный
Key Usage	AwIHgA==	<input checked="" type="checkbox"/>
Enhanced Key Usage	<автоматически>	<input checked="" type="checkbox"/>
Certificate Template Name	<автоматически>	<input checked="" type="checkbox"/>

После того как набор «Роли Шаблона» отредактирован, Администратор нажимает кнопку «Сохранить изменения».

Сохранить изменения

Затем возникает дополнительное окно подтверждения:

- ▶ Для сохранения изменений Администратору необходимо нажать кнопку «Сохранить на сервер».
- ▶ Для прерывания редактирования Администратору необходимо нажать кнопку «Отменить правку».

- Для возвращения к внесению изменений в шаблон Администратору необходимо нажать кнопку «Продолжить редактирование».

 Подтвердите действие

Сохранить изменения шаблона сертификата?

ПРОДОЛЖИТЬ РЕДАКТИРОВАНИЕ


ОТМЕНИТЬ ПРАВКУ

СОХРАНИТЬ НА СЕРВЕР

В случае если Администратор понимает отсутствие потребности в конкретном шаблоне, он может удалить его, нажав кнопку «Удалить шаблон».

Удалить шаблон

Для удаления шаблона Администратору потребуется подтвердить свои действия в открывшемся окне нажатием кнопки «Удалить».

 Подтвердите действие

Удалить шаблон сертификата?

ОТМЕНИТЬ

УДАЛИТЬ

В случае если удаление шаблона не требуется, Администратор нажимает кнопку «Отменить».

6.2. Настройка Справочников Центра Сертификации

На данный момент Администратору доступно два справочника:

- ▶ Справочник атрибутов сертификата;
- ▶ Справочник расширений использования ключей (EKU);
- ▶ Справочник имен субъекта.

Справочник атрибутов сертификата

Название атрибута Oid

Название атрибута	Oid	Действия
Certificate Template Name	1.3.6.1.4.1.311.20.2	5
Key Usage	2.5.29.15	
Certificate Template Information	1.3.6.1.4.1.311.21.7	
Application Policies	1.3.6.1.4.1.311.21.10	
Basic Constraints	2.5.29.19	

Элементов на странице: 1 – 5 из 6

Справочник расширений использования ключей (EKU)

Название Eku Oid

Название Eku	Oid	Действия
Microsoft Trust List Signing	1.3.6.1.4.1.311.10.3.1	
Encrypting File System	1.3.6.1.4.1.311.10.3.4	
Secure Email	1.3.6.1.5.5.7.3.4	
Client Authentication	1.3.6.1.5.5.7.3.2	
Server Authentication	1.3.6.1.5.5.7.3.1	

Элементов на странице: 1 – 5 из 10

Справочник имен субъекта

Название имени субъекта Oid

Название имени субъекта	Oid	Действия
C	2.5.4.6	
O	2.5.4.10	
T	2.5.4.12	
OJ	2.5.4.11	
CN	2.5.4.3	

Элементов на странице: 1 – 5 из 38

Администратор может изучить содержимое полей каждого справочника в таблице.

Название атрибута	Oid	Действия
Certificate Template Name	1.3.6.1.4.1.311.20.2	5
Key Usage	2.5.29.15	
Certificate Template Information	1.3.6.1.4.1.311.21.7	
Application Policies	1.3.6.1.4.1.311.21.10	
Enhanced Key Usage	2.5.29.37	
Basic Constraints	2.5.29.19	

1 Записей на странице: 1-6 из 6 3 2 4

Для настройки отображаемого количества записей справочника Администратор может выбрать необходимое количество (цифра 1).

Для переключения между страницами Администратор может воспользоваться ординарными стрелками (цифра 2).

Для быстрого перемещения на первую или последнюю страницу Администратор может воспользоваться крайними левой и правой стрелками соответственно (цифры 3 и 4).

Для удаления атрибута или расширения из справочника Администратору необходимо нажать кнопку корзины напротив выбранной позиции (цифра 5).

<input type="text" value="Название атрибута"/>	<input type="text" value="Oid"/>
<input type="button" value="ДОБАВИТЬ"/>	

Для добавления нового атрибута или расширения Администратору необходимо заполнить поле с названием, а также поле с соответствующим ему OID. После чего необходимо нажать кнопку «Добавить». Добавленная позиция появится в таблице справочника.

6.3. Настройка Email-рассылки

Администратор может настроить правила для уведомления пользователей Центра Сертификации об изменении статуса сертификатов, а также отредактировать и ознакомиться с уже существующими правилами.

[Настройки](#) - [Email рассылки](#)

<input type="text" value="Найти"/>	<input type="button" value="Создать правило рассылки"/>
<hr/>	
Название правила Email-рассылки	
<hr/>	
Выпуск на User ST_CA	

6.3.1. Создание нового правила для Email-рассылки

Для создания нового правила Администратору необходимо нажать кнопку "Создать правило рассылки".

Настройки правил Email-рассылки

Наименование правила
Новая рассылка от 2024-11-28_19:29:13

Текст уведомления

Выберите событие * Обязательное поле

Выберите шаблон * Обязательное поле

Адреса получателей
Добавьте адреса получателей

Адрес электронной почты

* Добавьте хотя бы один адрес или выберите отправление по указанному в сертификате адресу

Направлять письмо по адресу электронной почты, указанному в сертификате

Для настройки правила Администратору необходимо:

- указать название правила в поле "Наименование правила";
- (опционально) в поле "Текст уведомления" указать текст, который будет приходить получателю в теле письма;
- выбрать "Событие", в момент исполнения которого будет происходить отправка письма.
Доступны 4 возможных события:
 - сертификат выпущен - уведомления пользователя направляется в момент совершения события;
 - сертификат отозван - уведомления пользователя направляется в момент совершения события;
 - сертификат просрочен - уведомления пользователя направляется в момент совершения события;
 - сертификат истекает - Администратору потребуется указать время, за которое потребуется уведомить пользователя о приближающемся сроке истечения сертификата.

через 1 день через 5 дней

через 10 дней через 15 дней

через 30 дней

* Обязательное поле

Администратор может одновременно выбрать несколько значений.

Тема письма будет формироваться автоматически и будет включать в себя наименование выбранного события + серийный номер сертификата.

- выбрать "Шаблон" - таким образом, правило будет работать для запросов на выпуск сертификатов по указанному в правиле шаблону;

5. указать "Адреса получателей"

Администратор может поставить галочку в строке "Направлять письмо по адресу электронной почты, указанному в сертификате", и/или ввести адреса вручную.

После заполнения всех полей для сохранения правила Администратору необходимо нажать кнопку "Создать рассылку".

В случае если Администратор хочет прервать создание правила, необходимо нажать на кнопку "Отменить создание".

6.3.2. Редактирование правила для Email-рассылки

Для редактирование уже существующего правила Администратору необходимо выбрать его из списка, затем отредактировать поля. После чего нажать кнопку "Сохранить изменения".

6.3.3. Удаление правила для Email-рассылки

Для удаления уже существующего правила Администратору необходимо выбрать его из списка, затем нажать кнопку "Удалить рассылку".

7. Импорт шаблонов и сертификатов из Microsoft CA

Администратору доступна функциональность импорта шаблонов и сертификатов из уже существующего в организации Microsoft CA.

7.1. Импорт шаблонов из Microsoft CA

Для импорта шаблонов из Microsoft CA Администратору необходимо перейти в раздел "Настройка шаблонов" и нажать кнопку "Импортировать шаблоны".

Администратору необходимо указать данные для доступа к LDAP-каталогу с шаблонами Microsoft CA:

1. URL;
2. базовый DN;
3. DN пользователя;
4. Пароль.

ВВЕДИТЕ УЧЕТНЫЕ ДАННЫЕ

Пожалуйста введите учетные данные для импорта шаблонов из MS CA



После чего нажать кнопку "Импортировать". Указанные данные будут сохранены, Администратор всегда может вернуться к процессу импортирования шаблонов, не вводя данные повторно, для возврата к процессу импорта шаблона Администратору необходимо нажать кнопку "Импортировать с ранее введенными данными".

После указания корректных данных Администратор перейдет в режим импортирования шаблонов. Режим импортирования шаблонов состоит из двух разделов:

1. Готовые к импорту - раздел содержит в себе шаблоны, которые могут быть перенесены в Центр Сертификации без внесения корректировок.

Готовые к импорту

[ИМПОРТИРОВАТЬ ВСЁ](#)

Наименование шаблона сертификата

OfflineRouter

SmartcardUser

OCSPResponseSigning

SmartcardLogon

CTLSigning

ExchangeUser

DomainController

CrossCA

Administrator

UserSignature

Items per page:

10 ▼

1-10 of 24



Администратор может ознакомиться с содержанием каждого шаблона, открыв шаблон нажатием на него, внести в него корректировки. После чего импортировать шаблон нажатием кнопки "Импортировать шаблон".

Администратор может импортировать сразу все готовые к импорту шаблоны нажатием кнопки "Импортировать все".

2. Конфликты - раздел отображает ошибки, которые возникли с некоторыми из импортируемых шаблонов. Возможны два вида конфликтов:

- Расширения использования ключей (EKU) отсутствуют в справочнике расширений. Администратор может разрешить конфликты, указав названия расширений использования ключа перед соответствующими расширениями. Как только расширение будет добавлено в справочник, все шаблоны, содержащие в себе данное расширение будут автоматически перенесены в раздел готовых к импорту (в случае если конфликт был единственный, иначе шаблон будет готов к

импорту только после разрешения всех конфликтов).

Конфликты

Отсутствуют ЕКУ в словаре

Пожалуйста, добавьте недостающие ЕКУ

1.3.6.1.4.1.311.20.2.1

1.3.6.1.5.5.8.2.2

1.3.6.1.4.1.311.21.5

1.3.6.1.5.5.7.3.3

1.3.6.1.4.1.311.21.6

- Шаблоны с таким названием уже существуют. Для разрешения конфликта Администратор может открыть конфликтный шаблон и изменить его имя. После чего нажать кнопку "Импортировать шаблон". Шаблон автоматически будет импортирован в Центр Сертификации.

Шаблоны с таким названием уже существуют

Пожалуйста, измените названия шаблонов

Наименование шаблона сертификата

Copy of User

Items per page:

1-1 of 1



После того как все шаблоны будут импортированы, Администратору будет предложено перейти к импорту сертификатов.

7.2. Импорт сертификатов из Microsoft CA

Администратор может загрузить csv файл в окно, открывшееся сразу после импорта шаблонов или перейдя в раздел "Сертификаты" и нажав кнопку "Импортировать сертификаты".

 **ИМПОРТИРОВАТЬ СЕРТИФИКАТЫ**

Для импорта сертификатов Администратору необходимо экспортировать из Active Directory csv файл со всеми сертификатами, выпущенными в Microsoft CA.

Импорт сертификатов из Microsoft CA



Перед импортом сертификатов, убедитесь, что все шаблоны Microsoft CA уже импортированы.



Выберите файл с сертификатами

Импортировать сертификаты

Отмена

После чего Администратору необходимо нажать кнопку "Импортировать сертификаты", все сертификаты из загруженного csv файлы будут перенесены в Центр Сертификации.