РУТОКЕН

Рутокен KeyBox. Описание и применение

Содержание

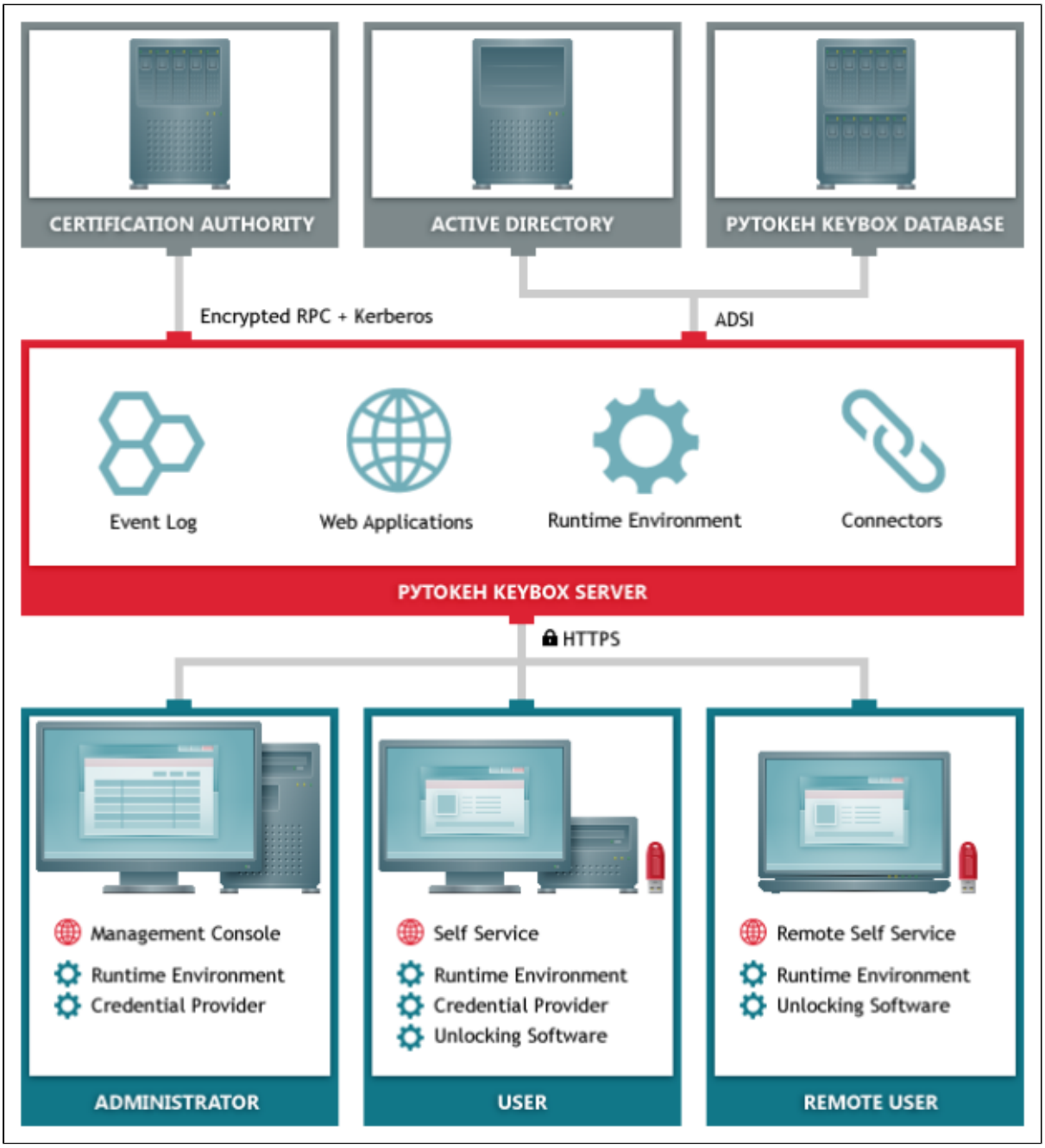
Раздел 1. Описание системы

Назначение системы

Система Рутокен KeyBox предназначена для внедрения, управления и учета аппаратных средств аутентификации пользователей в масштабах предприятия. Рутокен KeyBox обеспечивает централизованное управление средствами аутентификации в течение всего жизненного цикла, учет средств аутентификации и аудит их использования, быстрое и самостоятельное решение проблем пользователей без обращения к администраторам, в том числе за пределами предприятия.

Структура системы

Система состоит из серверной и клиентской частей.



Компоненты серверной части:

Ядро: Рутокен KeyBox Server — основной модуль системы.

Вспомогательные утилиты:

- Configuration Tool — мастер конфигурирования домена, создающий необходимую структуру каталогов в AD;
- Card Monitor — служба мониторинга смарт-карт.

Web-сервисы:

- Management Console — консоль администратора, позволяющая конфигурировать систему, работать с устройствами аутентификации пользователей, просматривать журнал операций системы;
- Self Service — консоль самообслуживания, позволяющая пользователям самостоятельно работать с устройствами аутентификации, привязанными к ним;
- Remote Self Service — консоль самообслуживания, позволяющая пользователям выполнять операции с устройствами аутентификации за пределами домена;
- Web API — веб-сервис управления жизненным циклом устройств аутентификации.

Компоненты клиентской части:

1. Рутокен KeyBox — Middleware (компонент, предоставляющий единый интерфейс остальным компонентам системы по управлению устройствами аутентификации, подключенными к рабочей станции пользователя).
2. Рутокен KeyBox — Client Tools:

- Credential Provider — компонент для разблокировки устройств, использующихся для аутентификации в операционной системе Windows, в offline- и online-режимах;
- PIN Reset Tool — компонент для offline разблокировки устройств.

В качестве средства хранения данных и настроек системы используется Active Directory.

Роли пользователей

В системе определены три пользовательские роли:

- Администраторы системы — обладают полными правами на управление пользователями, устройствами аутентификации, а так же управление системой и изменение ее конфигурации.
- Операторы службы поддержки — обладают правами на управление картами пользователей, без возможности изменения конфигурации системы.
- Пользователи системы — обладают правами на управление своими картами.

Managment Console

Модуль, позволяющий конфигурировать систему, работать с устройствами аутентификации пользователей, просматривать журнал операций системы. Реализован в виде WEB-приложения.
Работу с данным модулем ведет администратор системы и сотрудники службы технологической поддержки.

Web-приложение состоит из следующих разделов:

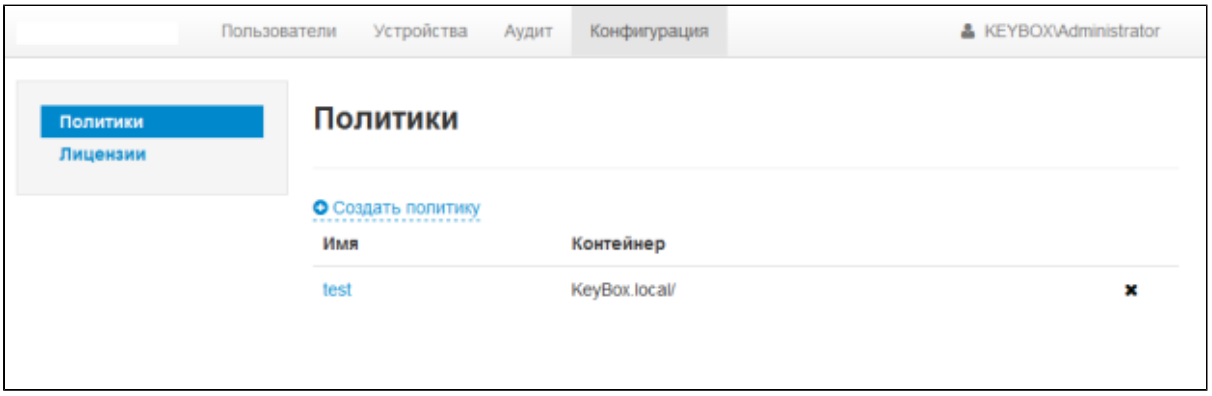
1. Пользователи.
2. Устройства.
3. Аудит.
4. Конфигурация.

Для доступа к приложению используется доменная аутентификация.

Раздел "Конфигурация"

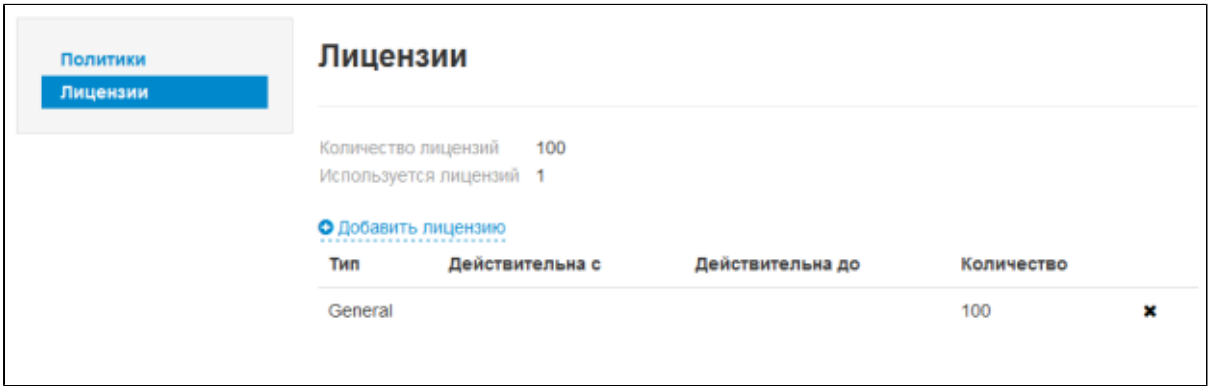
Раздел состоит из следующих подразделов:

1. Политики — предназначен для установки основных настроек системы.
2. Лицензии — предназначен для управления лицензиями системы.



Лицензии

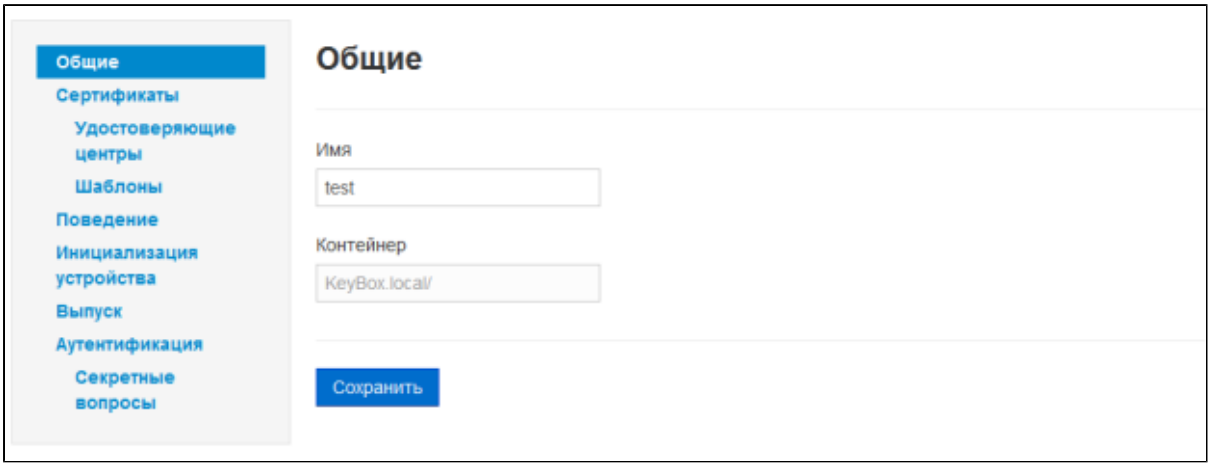
Лицензии распространяются в виде файла лицензий. Для начала работы необходимо добавить лицензию в систему в разделе Конфигурация.



Учет лицензий ведется следующим образом:
При назначении первой карты пользователю лицензия захватывается. В случае изъятия всех карт у пользователя лицензия отзывается. Количество занятых лицензий и общее количество можно просмотреть в подразделе "Лицензии" .

Политики

Политика задает основные правила и возможности работы пользователя с системой, УЦ, с которым взаимодействует пользователь, набор сертификатов, выписываемых при выпуске устройства.



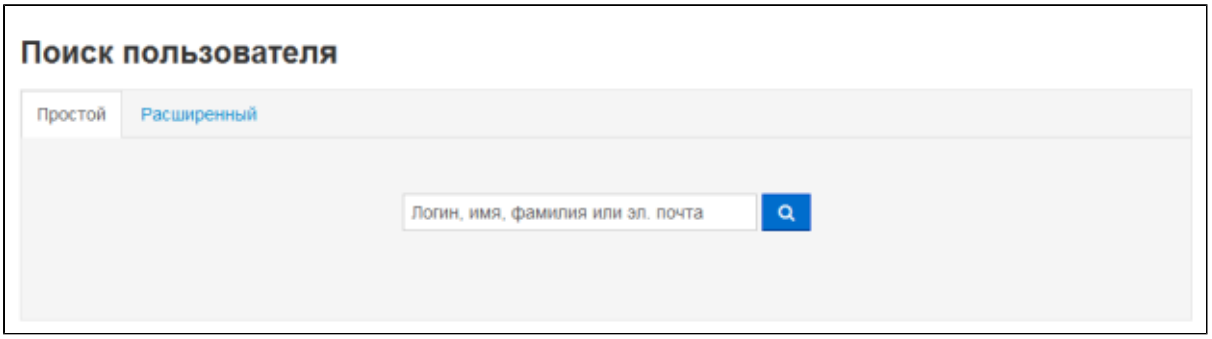
Политика действует на все учетные записи, хранящиеся в контейнере, на который она распространяется. Политика включает в себя следующие группы настроек:

- Общие настройки включают в себя имя политики и область действия, область действия задается при создании и не может быть изменена.
- Сертификаты — группа настроек, включающих в себя настройки центров сертификации, шаблонов сертификатов для использования в системе, параметры выпуска и использования сертификатов.
- Поведение — группа настроек, задающих правила работы пользователей с устройствами.
- Инициализация устройств — группа настроек, задающих параметры инициализации устройств.
- Выпуск — настройки параметров выпуска карты.
- Аутентификация — группа настроек, устанавливающих правила аутентификации пользователей в системе.

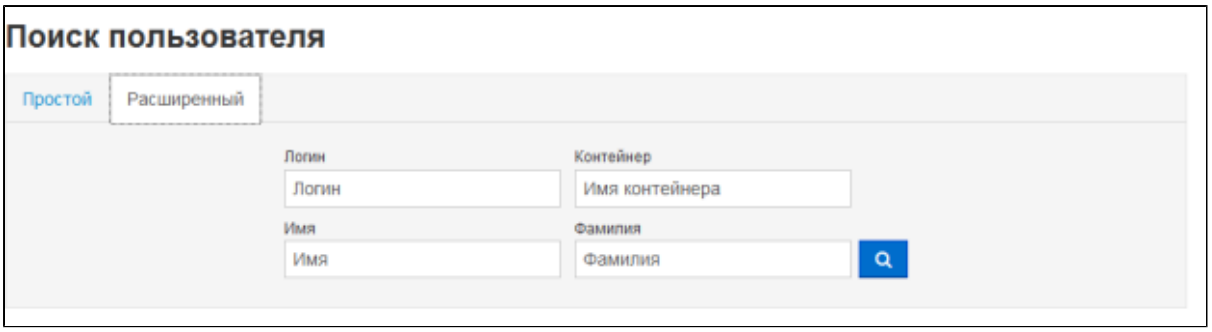
Раздел "Пользователи"

Данный раздел позволяет осуществлять поиск пользователей и работу с их устройствами аутентификации. Список пользователей берется из AD.
Реализовано два типа поиска:

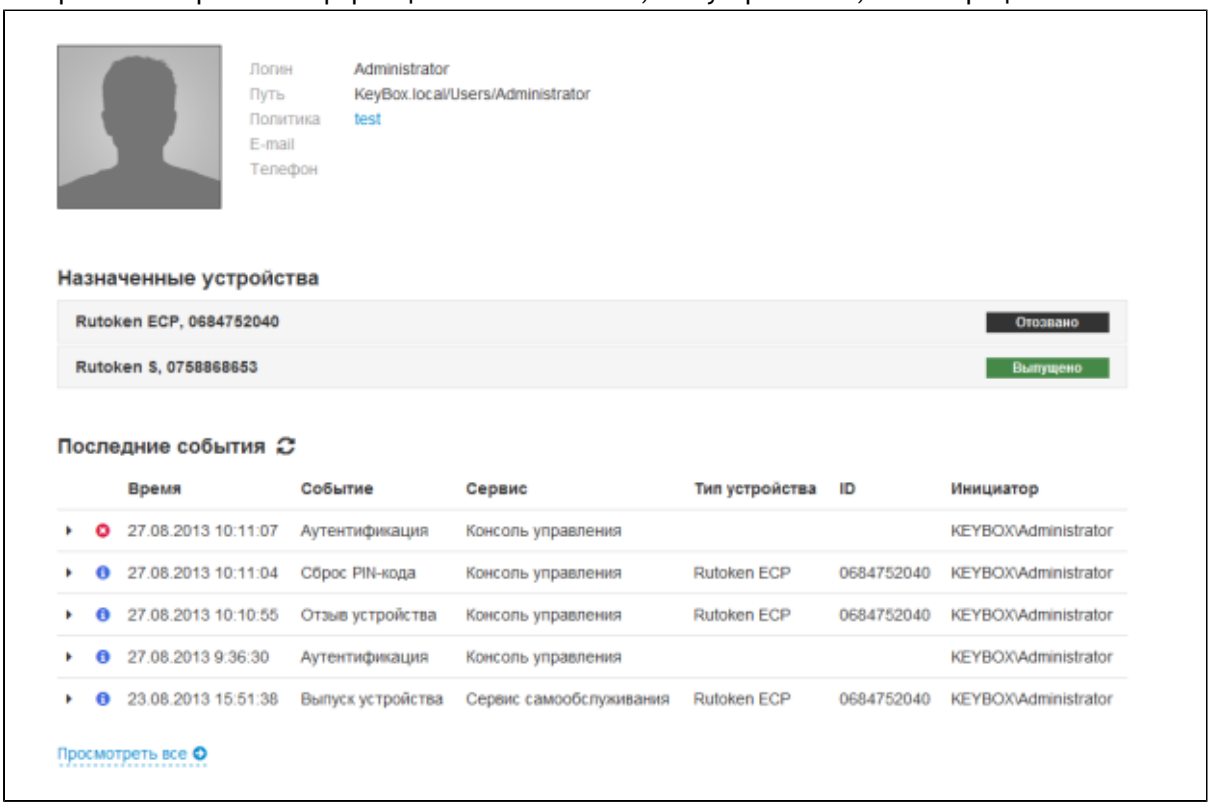
- «Простой» поиск осуществляется по любому из следующих атрибутов учетной записи пользователя: логин, имя, фамилия, e-mail.



- Расширенный поиск возможен по набору атрибутов: логин, имя, фамилия, контейнер, в котором хранится учетная запись в AD.



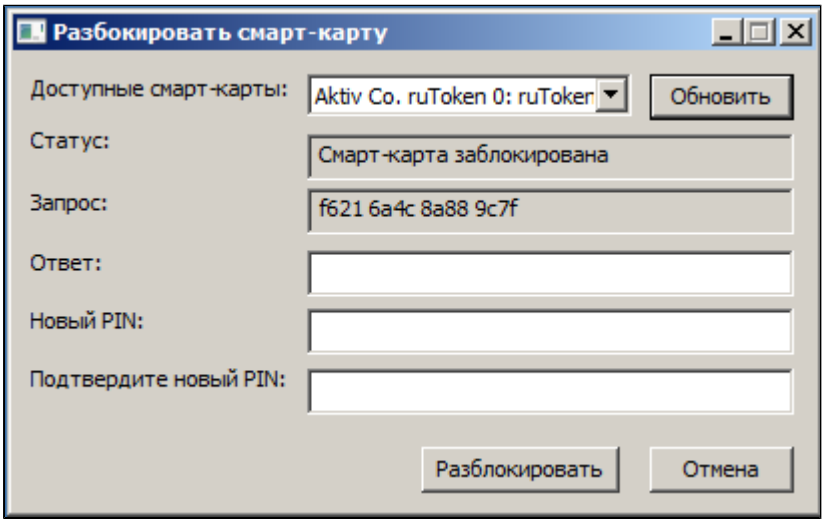
Работа с устройствами аутентификации пользователя ведется через карточку пользователя. В карточке отображается краткая информация о пользователе, его устройствах, его операциях в системе.



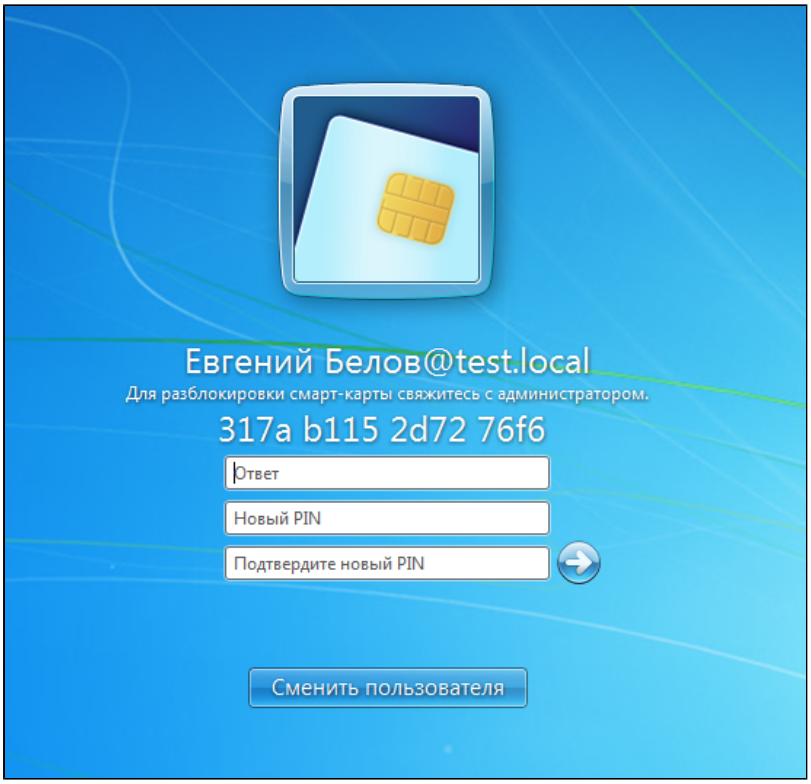
В карточке пользователя доступны следующие операции:

- Назначение устройства — привязка устройства, имеющегося в системе, к учетной записи без выпуска устройства. После назначения выпуск производится пользователем самостоятельно в личном кабинете.
- Выпуск устройства — привязка устройства к ученой записи пользователя и выпуск всех необходимых сертификатов. После выпуска устройство полностью готово к использованию.
- Сброс PIN-кода — изменение PIN-кода устройства на PIN-код по умолчанию, в случае если пользователь забыл свой PIN-код. Для проведения данной операции необходимо устройство аутентификации.

- Разблокировка устройства — разблокировка PIN-кода устройства, в случае если он был неверно введен установленное количество раз. Разблокировка может производиться в режиме offline, если данная опция разрешена для пользователя, устройство которого было заблокировано.В случае offline разблокировки пользователь, используя PIN Reset Tool, генерирует запрос и передает его сотруднику технической поддержки, который на его основе генерирует ответ. Пользователь вводит ответ в PIN Reset Tool, указывает новый PIN-код и разблокирует устройство.

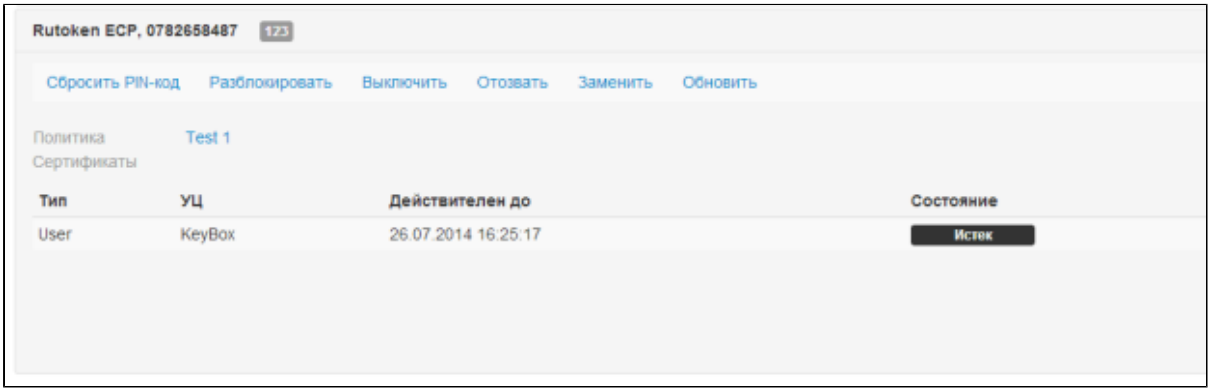


Если пользователь заблокировал устройство при попытке войти в домен, то разблокировка производится посредством Credential Provider. При превышении заданного числа попыток ввода PIN-кода пользователь получает сообщение о том, что его устройство заблокировано и запрос.



Получив ответ от сотрудника технической поддержки, пользователь вводит его в соответствующее поле, указывает новый PIN-код, подтверждает новый PIN-код и завершает разблокировку устройства.

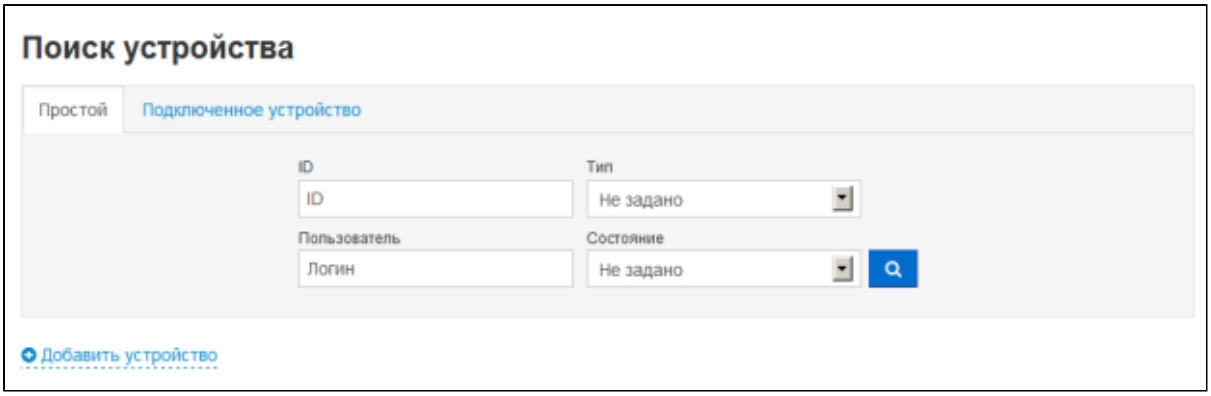
- Выключение\Включение устройства — временный отзыв сертификатов пользователя, выданных в системе. Выключить или включить устройство может либо пользователь, либо сотрудник технической поддержки, в зависимости от настроек для данного пользователя.
- Замена устройства — временная или постоянная замена устройства пользователя на новое.При временной смене устройства пользователю выписываются новые сертификаты, при этом старые временно отзываются (на срок действия новых).При постоянной замене сертификаты на старом устройстве пользователя отзываются без возможности восстановления.
- Отзыв устройства может производиться по ряду причин: неисправность устройства, утеря устройства, обновление устройства, изъятие устройства.
- Обновление устройства — обновление сертификатов на устройстве (доступно, если до окончания срока сертификата осталось меньше 10 % времени его действия).В процессе отзыва будут отозваны все сертификаты пользователя, выданные системой. Устройство будет переведено в состояние «Отозвано», пользователю станут недоступны операции с устройством.
- Разблокировка пользователя — снятие блокировки с учетной записи пользователя, если она была заблокирована. В случае, если учетная запись пользователя была заблокирована, пользователь теряет доступ к удаленному личному кабинету.



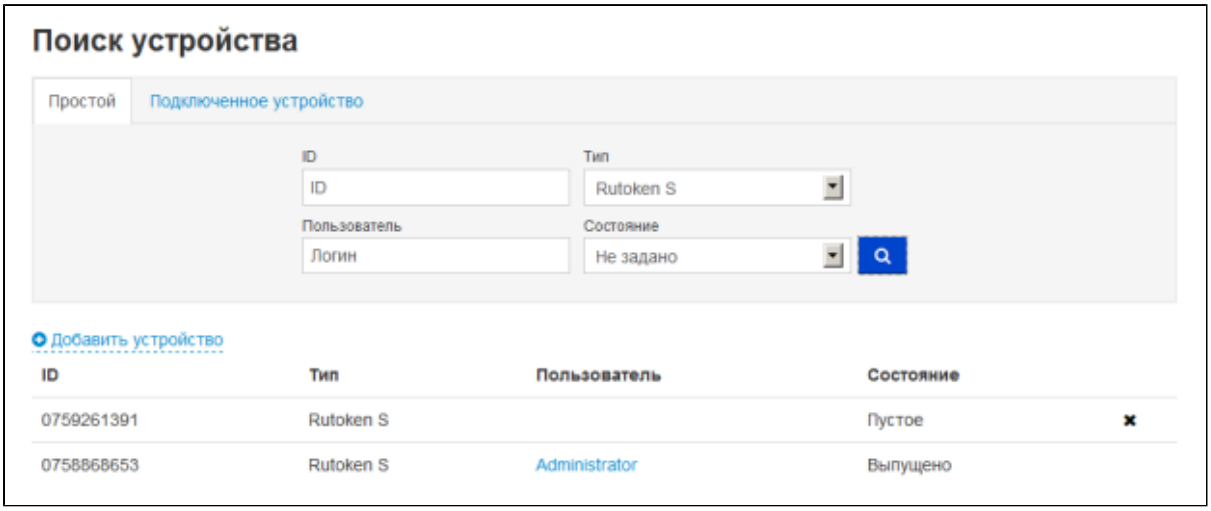
Помимо операций с устройством в карточке пользователя можно просмотреть список последних операций пользователя в системе.

Раздел "Устройства"

Данный раздел позволяет производить добавление новых устройств в систему и поиск устройств, зарегистрированных в системе.
В разделе доступны 2 типа поиска: поиск по параметрам (ID устройства, тип, логин пользователя, которому назначено данное устройство, состояние устройства) и поиск по подключенному устройству.



В результате поиска выводится таблица, в которой содержится следующая информация об устройстве: ID; модель устройства; пользователь, которому назначено данное устройство; состояние устройства.

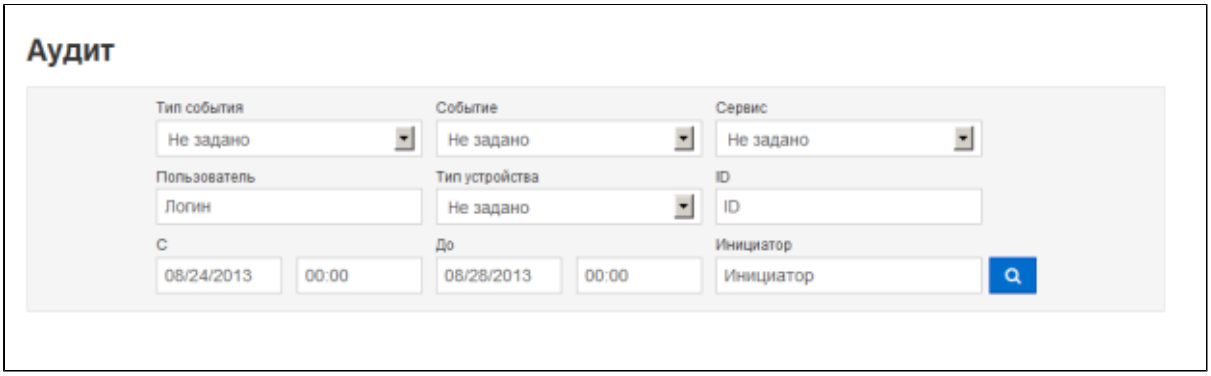


При необходимости произвести операцию с найденным устройством из результатов поиска можно перейти к карточке пользователя, которому назначено данное устройство.

Также в данном разделе производится изъятие отозванного устройства у пользователя. В результате операции изъятия выполняется отмена назначения устройства пользователю. В карточке пользователя информация об устройстве больше не отображается, теперь устройство можно удалить из системы.

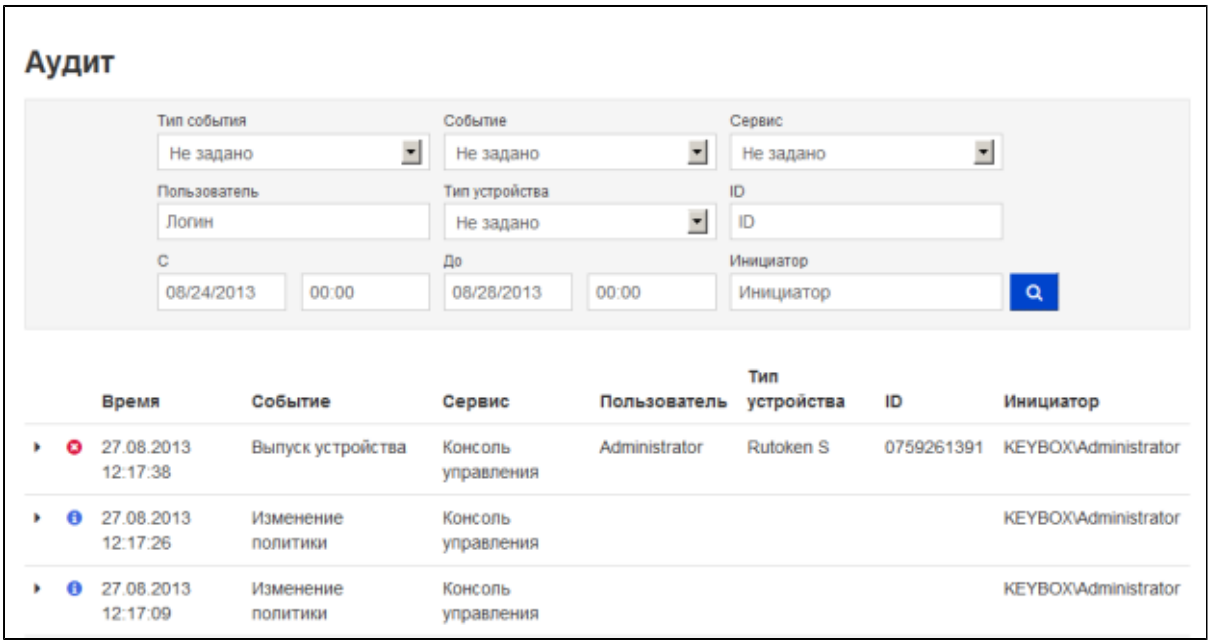
Раздел "Аудит"

Раздел предназначен для просмотра журнала операций системы.



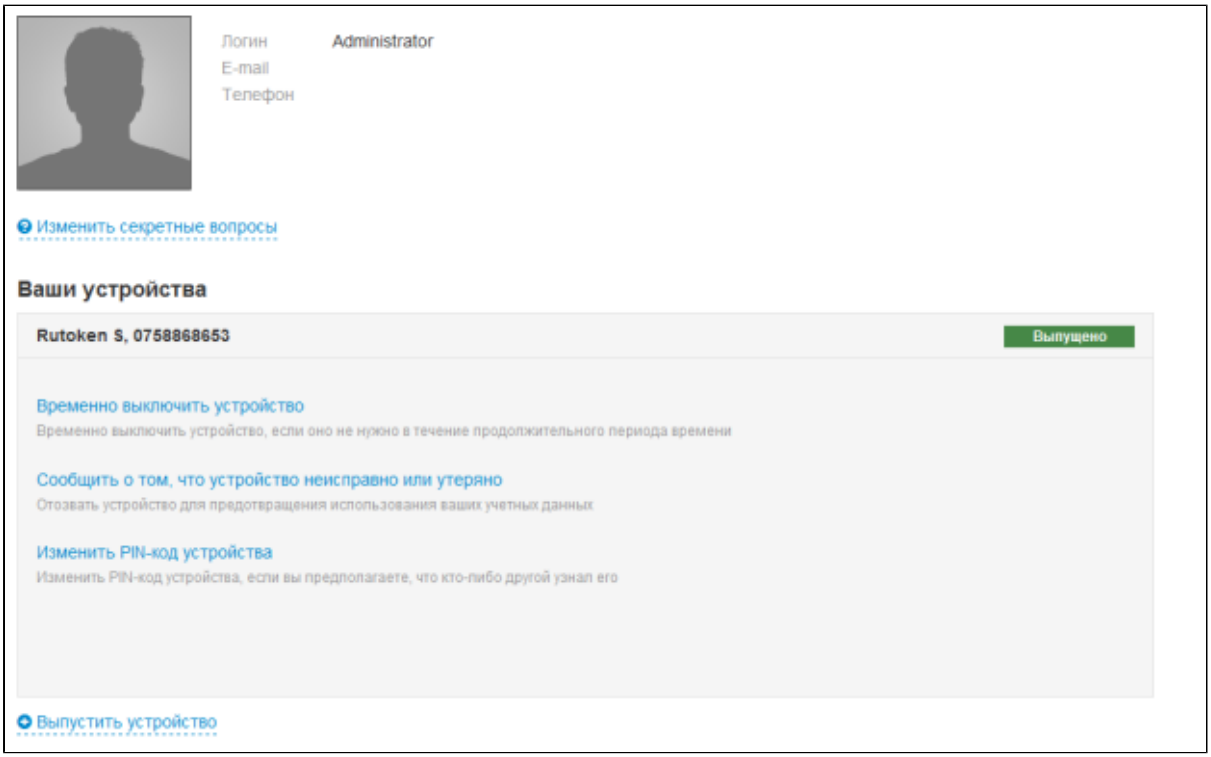
Для удобства использования в разделе реализованы фильтры по следующим атрибутам события:

- Тип события — информация (сообщение об успешном завершении события), ошибка, предупреждение.
- Событие — произведенная операция.
- Сервис — раздел системы, с помощью которого была произведена операция.
- Пользователь — логин пользователя, с учетной записью которого производилась операция.
- Тип устройства — тип устройства аутентификации.
- ID - ID устройства аутентификации.
- Временной интервал.
- Инициатор - пользователь, проводивший операцию.



Self Service

Web-приложение, позволяющее пользователям производить операции с устройствами аутентификации без помощи сотрудников технической поддержки. Количество доступные операции с устройствами зависит от настроек, установленных в политике, применяющейся к данному пользователю.

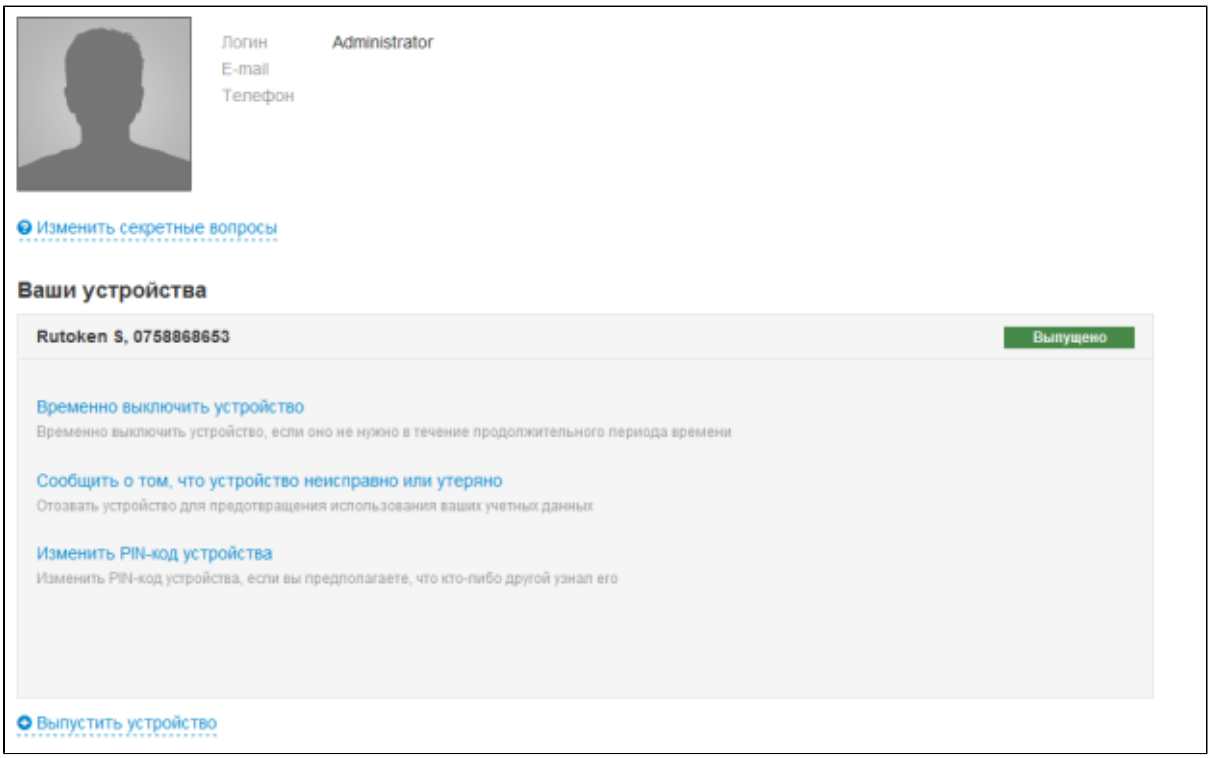


Для доступа к приложению используется доменная аутентификация.
В личном кабинете пользователю доступны следующие операции:

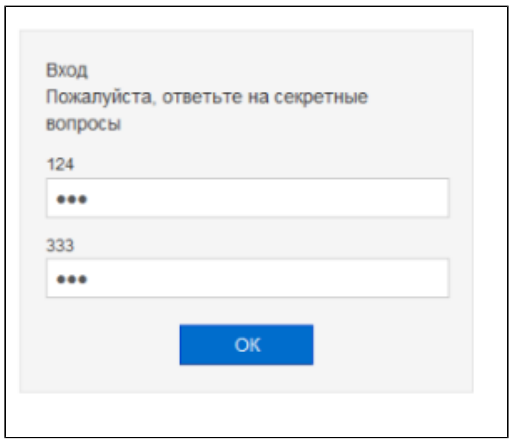
- Выпуск устройства.
- Временное выключение\включение устройства. При временном выключении устройства, временно отзываются сертификаты пользователя, используемые в системе.
- Изменение PIN-кода.
- Сброс PIN-кода.
- Изменение секретных вопросов. Пользователь может изменять ответы на секретные вопросы или список вопросов. Секретные вопросы применяются для проведения ряда операций в личном кабинете: offline разблокировки устройства, доступа к удаленному личному кабинету.

Remote Self Service

Внешнее Web-приложение, предназначенное для работы пользователей с устройствами аутентификации за пределами домена. Список доступных операций зависит от настроек политики.



Доступ предоставляется после ввода имени пользователя и ответов на секретные вопросы.



В удаленном личном кабинете пользователю доступны следующие операции:

- Временное выключение\включение устройства.
- Отзыв устройства в случае утери или поломки.
- Разблокировка устройства (требует наличия утилиты PIN Reset Tool).

Раздел 2. Установка и настройка

Системные требования

Серверная часть

Аппаратные требования

Минимальные:

- Intel Pentium D 2.5 ГГц;
- 1 ГБ RAM;
- 100 МБ свободного пространства на системном диске.

Рекомендуемые:

- Intel Core 2Duo 2.5 ГГц;
- 2 ГБ RAM;
- 50 ГБ сбодного пространства на системном диске.

Поддерживаемые операционные системы

- Windows Server 2008 Standart/Enterprise/Datacenter SP2 32/64bit (с обновлением KB980368).
- Windows Server 2008 R2 Standart/Enterprise/Datacenter SP1.
- Windows Server 2012 Standart/Enterprise/Datacenter.
- Windows Server 2012 R2 Standart/Enterprise/Datacenter.

Требования для установки Rutoken KeyBox Server

Web-сервер IIS:

- Internet Information Services 7.0 и выше.
- Роль Web Server (Internet Information Services) и установленные службы: Microsoft .NET и выше[1]

- перенаправление HTTP (HTTP Redirection);

- ASP.NET;

- расширяемость .NET (.Net Extensibility);

- расширения ISAPI (ISAPI Extensions);

- фильтры ISAPI (ISAPI Filters);

- обычная проверка подлинности (Basic Authentication);

- Windows-проверка подлинности (Windows Authentication);

- КриптоПРО CSP 3.6R4 и 3.9[2]

[1] При развертывании сервера Rutoken KeyBox необходимо выполнить установку Microsoft .NET 4.5 после установки и настройки компонента IIS.

[2] Для использования с КриптоПРО УЦ. В случае использования TSL-соединения между сервером Rutoken KeyBox и Центром Регистрации КриптоПРО, зищищенного в соответствии с Государственными Стандартами РФ, необходимо наличие серверной лицензии КриптоПРО.

Требования к окружению

Центры сертификации:

- Центр сертификации предприятия Microsoft (Microsoft Enterprise CA) 2003- 2012R2.
- Центр сертификации КриптоПРО 2.0 RC5 сборка 2.0.5439.0200.
- Центр сертификации КриптоПРО 1.5 R2 SP1.

Поддерживаемые типы хранилища данных:

- Active Directory без расширения схемы.
- База данных SQL:

- Microsoft SQL Server 2012 SP2 Express/Standart;

- Microsoft SQL Server 2014 TP.

Клиентская часть

Аппаратные требования

Минимальные:

- Intel Celeron 500 МГц;
- 256 МБ RAM;
- 30 МБ свободного места на жестком диске;
- USB-порт (для аппаратных ключей). Для смарт-карт других типов необходимо наличие установленного соответствующего считывателя.

Рекомендуемые:

- Intel Pentium 4 1.5 ГГц;
- 1 ГБ RAM;
- 30 МБ свободного места на жестком диске;
- USB-порт (для аппаратных ключей). Для смарт-карт других типов необходимо наличие установленного соответствующего считывателя.

Поддерживаемые операционные системы

- Windows Vista SP2 32/64bit.
- Windows 7 SP0/SP1 32/64bit.
- Windows 8 32/64bit.
- Windows 8.1 32/64bit.
- Windows Server 2008 Standart/Enterprise/Datacenter SP2 32/64bit (с обновлением KB980368).
- Windows Server 2008 R2 Standart/Enterprise/Datacenter SP1.

- Windows Server 2012 Standart/Enterprise/Datacenter.
- Windows Server 2012 R2 Standart/Enterprise/Datacenter.

Требования к окружению

- Установленные драйверы используемых устройств аутентификации.
- Internet Explorer 9 и выше.
- КриптоПРО CSP (В случае использования с КриптоПРО УЦ).

Поддерживаемые устройства аутентификации

- Рутокен S;
- Рутокен ЭЦП;
- Рутокен Lite;
- KAZTOKEN ;
- eToken Pro 64k;
- eToken Pro Java 72k;
- ePass 2003 (EC,RSA);
- Avest Key-256-A.

Порядок установки и настройки

Порядок установки и настройки Rutoken KeyBox зависит от окружения, в котором планируется эксплуатировать систему. Данные системы Rutoken KeyBox могут храниться как в Active Directory, так и в базе данных SQL. Пользователи системы могут быть расположены в Active Directory и Центрах Регистрации КриптоПро УЦ 1.5 и 2.0. Исходя из этого, можно выделить следующие конфигурации:

- Хранилище данных Rutoken KeyBox и каталог пользователей в Active Directory с использованием удостоверяющих центров Microsoft CA, КриптоПро УЦ 1.5 и КриптоПро УЦ 2.0.
- Хранилище данных Rutoken KeyBoxв базе SQL и каталог пользователей в Центре Регистрации КриптоПро 1.5 с использованием удостоверяющих центров КриптоПро УЦ 1.5 и КриптоПро УЦ 2.0.
- Хранилище данных Rutoken KeyBoxв базе SQL и каталог пользователей в Центре Регистрации КриптоПро 1.5 с использованием удостоверяющих центров КриптоПро УЦ 1.5 и КриптоПро УЦ 2.0.

Наглядно типовые конфигурации представлены в таблице.

	Хранилище Rutoken KeyBox	**Каталог пользователей**	**Удостоверяющие центры**
1	Active Directory	Active Directory	Microsoft CA, КриптоПро УЦ 1.5 и 2.0
2	SQL	Центр Регистрации КриптоПро УЦ 1.5	КриптоПро УЦ 1.5 и 2.0
3	SQL	Центр Регистрации КриптоПро УЦ 1.5	КриптоПро УЦ 1.5 и 2.0

Хранилище данных и каталог пользователей расположены в Active Directory

Установка серверной части

Установка Рутокен KeyBox Server

Запустите файл **KeyBox.Server.msi** из дистрибутива Рутокен KeyBox и выполните установку, следуя указаниям мастера.

Создание хранилища в Active Directory

Хранилище данных системы Рутокен KeyBox в Active Directory создается при помощи утилиты **KeyBox.StorageAD.exe** (располагается в KeyBox.Server\Misc\ дистрибутива).

Важная информация

В общем случае, для создания хранилища при помощи утилиты **KeyBox.StorageAD.exe** в корне домена необходимо наличие прав Администратора Домена (Domain Admins), либо администратор домена может создать вручную подразделение (Organizational Unit) с произвольным именем и предоставить полный доступ на управление этим подразделением и всеми его дочерними объектами выбранной учетной записи пользователя, от имени которой будет запущена утилита **KeyBox.StorageAD.exe**.

Для создания хранилища данных запустите утилиту **KeyBox.StorageAD.exe** из дистрибутива с параметром **/create <LDAP Path> "container name" "subcontainer name"**, где

<LDAP Path> – путь к контейнеру/подразделению домена, в котором необходимо создать хранилище,

"container name" – имя контейнера, в котором будут храниться все данные системы,

"subcontainer name" – имя подконтейнера, в котором будут созданы группы безопасности Рутокен KeyBox.

Ниже приведен пример запуска команды для создания хранилища данных в домене **KeyBox.local** с именем контейнера **Rutoken** и подконтейнером **KeyBox**.

KeyBox.StorageAD.exe /create LDAP://DC=KeyBox,DC=local Rutoken "KeyBox"

В результате работы утилиты в заданном контейнере будет создана следующая структура:

- Rutoken
  - KeyBox
    - Card Types
    - Card
    - Licenses
    - Policies
    - Users

Важная информация

Если указанные контейнеры не отображаются, необходимо включить опцию **Дополнительные компоненты** (Advanced Features). Для этого в **Active Directory Users and Computers** выберите пункт меню **Вид** (View) – **Дополнительные компоненты** (Advanced Features)

В контейнере KeyBox так же будут созданы группы безопасности:

Группа	Описание	Пользователи
KeyBox Admins	Члены группы обладают полными правами на управление системой Рутокен KeyBox (конфигурирование системы, изменение пользовательских настроек, управление устройствами идентификации)	Администраторы системы
KeyBox Help Desk Operators	Члены группы обладают правами на управление устройствами идентификации	Сотрудники технической поддержки
KeyBox Users	Члены группы обладают правами на использование приложений Self Service и Remote SelfService.	Пользователи системы

Важная информация

Имена групп безопасности зависят от имени контейнера, в котором они расположены. Например, если имя контейнера Test, то группы безопасности будут называться Test Admins, Test Help Desk Operators, Test Users.

Настройка системы для использования с УЦ Microsoft

Создание сервисных учетных записей

Для полноценной работы системы **Рутокен KeyBox** необходимо наличие определенных прав доступа к объектам **Active Directory** и **Центрам сертификации**. В соответствии с принятой в вашей компании политикой безопасности, Вы можете распределить привилегии между несколькими сервисными учетными записями, либо создать сервисную учетную запись с максимальным набором прав на управление системой.

При распределении привилегий, необходимо создать учетные записи.

Учетная запись пользователя (например, **serviceKeyBox**) для работы с контейнером **KeyBox**, от имени которой будут выполняться операции сохранения данных в **Active Directory**.
Выдайте данной учетной записи следующие полномочия: полные права (Full Control) на контейнер **KeyBox** и все его дочерние объекты.

Учетная запись пользователя (например, **serviceAD**), от имени которой система будет читать и вносить изменения в профили учетных записей пользователей.
Выдайте данной учетной записи следующие полномочия: права на чтение всех свойств пользователей, а также права на запись атрибута **userAccountControl** пользователям.

Для этого выполните следующие действия:

1. Откройте свойство **Безопасность** (Security) контейнера, в котором содержатся пользователи системы Рутокен KeyBox.
2. Нажмите **Добавить** (Add) и качестве пользователя укажите сервисную учетную запись.
3. Нажмите **Дополнительно** (Advanced), выберите сервисную учетную запись и нажмите **Изменить** (Edit).
4. Выберите область применения **Дочерние объекты: Пользователь** (Descendant User objects).
5. Перейдите на вкладку **Свойства** (Properties).
6. Выберите область применения **Дочерние объекты: Пользователь** (Descendant User objects).
7. Поставьте разрешение напротив **Прочитать все свойства** (Read all properties).
8. Поставьте разрешения для пунктов: **Запись: userAccountControl** (Write: userAccountControl).
9. Нажмите **ОК** и затем **Применить** (Apply).

Важная информация

Наличие данной сервисной учетной записи необходимо, только в том случае, если Вы планируете вносить изменения в профиль пользователя **Active Directory** посредством системы Рутокен KeyBox (использование опции "Требовать логон по смарт-карте" в разделе Настройки PKI).

Если пользователи размещены в нескольких контейнерах или подразделениях домена, необходимо для всех контейнеров/подразделений установить одинаковые права для сервисной учетной записи.

Учетная запись пользователя (например, **serviceCA**), от имени которой система будет запрашивать сертификаты пользователей в центре сертификации.
Выдайте данной учетной записи следующие полномочия: права на работу с центром сертификации.

Для этого выполните следующие действия:

1. Откройте оснастку **Центр сертификации** (Certification Authority), выберите центр сертификации и перейдите в его **Свойства** (Properties).
2. На вкладке **Безопасность** (Security) нажмите **Добавить** (Add).
3. В качестве пользователя укажите сервисную учетную запись.
4. Для выбранной учетной записи укажите разрешения на **Выдачу и управление сертификатами** (Issue and Manage Certificates) и сохраните настройки, нажав **ОК**.
5. Перейдите в раздел **Шаблоны сертификатов** (Certificate Templates) в дереве консоли **Центр сертификации** (Certification Authority), щелкните правой кнопкой мыши выберите **Управление** (Manage).
6. В свойствах безопасности шаблона **Агент регистрации** (Enrollement Agent) добавьте сервисную учетную запись и назначьте для нее права на **Чтение** (Read) и **Заявка** (Enroll). Выдайте аналогичные права для всех шаблонов сертификатов, которые будут использоваться системой Рутокен KeyBox. Например, для шаблона **Вход со смарт-картой** (Smartcard Logon), который будет использоваться для выпуска сертификатов, предназначенных для входа в операционную систему по смарт-карте.

Важная информация

Если в вашем окружении используется более одного центра сертификации, то сервисной учетной записи необходимо выдать одинаковый набор привилегий для всех центров сертификации.

Добавление шаблонов сертификатов в Центр Сертификации

Важная информация

Прежде, чем приступить к настройке Центра Сертификации для работы с системой Рутокен KeyBox, обратите внимание на размер ключей шифрования указанный в свойствах шаблонов сертификатов, которые Вы планируете использовать.

Чтобы снизить риск несанкционированного доступа к конфиденциальной информации компания Майкрософт выпустила несвязанное с безопасностью обновление (KB 2661254) для всех поддерживаемых версий Microsoft Windows. Это обновление блокирует криптографические ключи меньше 1024 бит. Это обновление не относится к Windows 8 или Windows Server 2012, потому что эти операционные системы уже могут блокировать использование слабых ключей RSA меньше 1024 бит. Подробная информация об этом обновлении содержится на сайте службы поддержки компании Майкрософт http://support.microsoft.com/kb/2661254

Для добавления шаблонов сертификатов в Центре сертификации:

1. Откройте оснастку **Центр Сертификации** (Certification Authority) и дважды щелкните имя ЦС.
2. Кликните правой кнопкой мыши на контейнере **Шаблоны сертификатов** (Certificate Templates), выберите команду **Создать** (New), а затем пункт **Выдаваемый шаблон сертификата** (Certificate Template to Issue).
3. Обязательно выберите шаблон сертификата **Агент регистрации** (Enrollment Agent), а также все остальные шаблоны сертификатов, которые будут использоваться системой Рутокен KeyBox, и нажмите **ОК**.

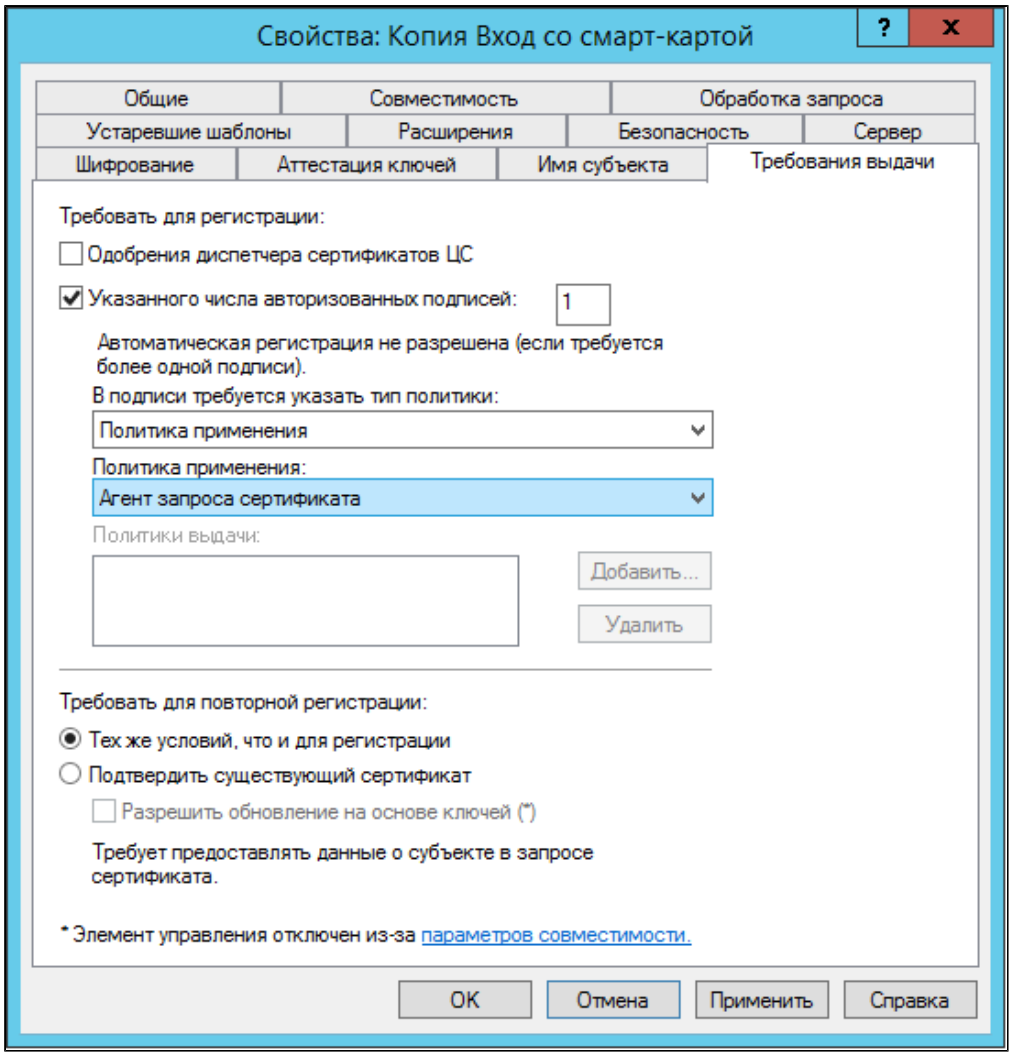
Важная информация

Для тех шаблонов сертификатов, которые были созданы через копирование, на основе оригинальных шаблонов, необходимо указать дополнительные настройки.

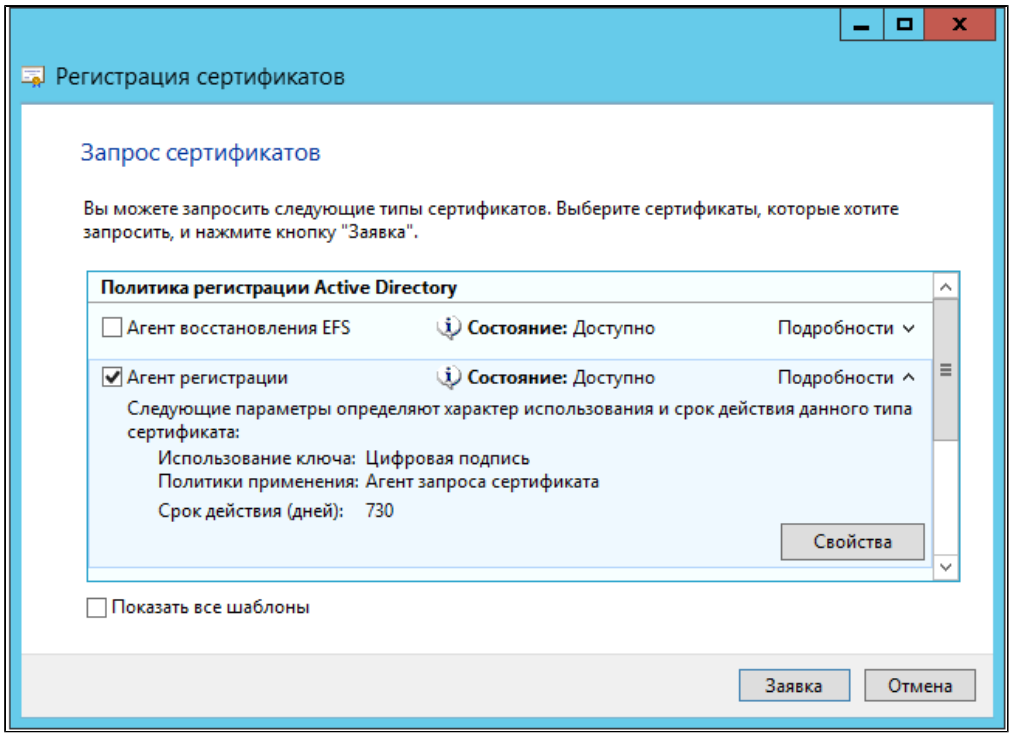
Дополнительные настройки дубликатов шаблонов сертификатов

Для указания дополнительных настроек:

1. Откройте свойства шаблона сертификата и перейдите на вкладку **Требования выдачи** (Issuance Requirements)
2. Отметьте опцию **Требовать для регистрации: Указанного числа авторизованных подписей** (This number of authorised signatures) и укажите число подписей, равное 1 (значение по умолчанию).
3. Установите значения политик: **Политика применения** (Application Policy) и **Агент запроса сертификата** (Certificate Request Agent).



4. В случае, если необходимо использовать секретный ключ какой-либо определенной длины, укажите необходимую длину ключа на вкладке **Обработка запроса** (Request Handling) в поле **Минимальный размер ключа** (Minimum key size).
5. На вкладке **Имя субъекта** (Subject Name) отключите опции **Включить имя электронной почты в имя субъекта** (Include e-mail name in subject name) и **Имя электронной почты** (E-mail name) в свойствах шаблона сертификата, если требуется выпуск сертификата пользователям, у которых не указан E-mail в учетных данных.



Выпуск сертификата Enrollment Agent

Наличие в системе Рутокен KeyBox пользователя, обладающего сертификатом **Агент регистрации** (Enrollment Agent) необходимо для того, чтобы от имени этого пользователя системой запрашивались сертификаты для всех пользователей. Сертификат может быть создан при помощи утилиты, поставляемой вместе с дистрибутивом Рутокен KeyBox (располагается в KeyBox.Server\Misc\), либо вручную, стандартными средствами Microsoft Windows

Выпуск сертификата при помощи утилиты KeyBox.CertEnroll.exe

Для выпуска сертификата с назначением **Агент регистрации** (Enrollment Agent) запустите от имени учетной записи с правами локального администратора на сервере Рутокен KeyBox утилиту **KeyBox. CertEnroll.exe** с параметром **/e <service username> <Password>**, где

<service username> – имя сервисной учетной записи для работы с центрами сертификации (“serviceCA”),

<Password> – пароль сервисной учетной записи.

Пример:

KeyBox.CertEnroll.exe /e serviceCA Password1

Результат работы утилиты:

DumpVariantStringWorker: 0: "Microsoft Enhanced Cryptographic Provider v1.0"

DumpVariantStringWorker: 1: "Microsoft Base Cryptographic Provider v1.0"

DumpVariantStringWorker: 2: "Microsoft Base DSS Cryptographic Provider"

CA: KeyBoxSrv.test.local\test-KeyBoxSrv-CA

'EnrollmentAgent' certificate has been enrolled successfully.

Если запрос на сертификат должен быть одобрен оператором УЦ, то утилита предложит принять запрос и продолжить работу, указав при этом порядковый номер запроса и имя ключевого контейнера:

CA: KeyBoxSrv.test.local\test-KeyBoxSrv-CA

Certificate request is pending.

Request id: 27

Container name: lr-EnrollmentAgent-175d9490-7481-4a29-b567-503d39747354

Please accept request and then install certificate.

После одобрения запроса оператором необходимо выполнить команду для установки сертификата в хранилище. Для этого запустите утилиту **KeyBox.CertEnroll.exe** с параметром **/i <service username> <Password> <requestId> <containerName>**, где:

<service username> – имя сервисной учетной записи для работы с центрами сертификации (“serviceCA”);

<Password> – пароль сервисной учетной записи;

<requestId> – порядковый номер запроса на сертификат;

<containerName> – имя ключевого контейнера

Пример:

KeyBox.CertEnroll.exe /e serviceCA password1 27 lr-EnrollmentAgent-175d9490-7481-4a29-b567-503d39747354

Результат работы утилиты:

CA: KeyBoxSrv.test.local\test-KeyBoxSrv-CA

Certificate has been installed successfully.

В результате работы утилиты в хранилище сертификатов компьютера, на котором установлен сервер Рутокен KeyBox, появится сертификат с назначением **Агент запроса сертификатов** (Enrollement Agent) с экспортируемым закрытым ключом и настроенными правами на управление закрытым ключом для учетной записи сервисного пользователя.

В случае необходимости можно указать имя шаблона сертификата (по умолчанию – Enrollment Agent) и центр сертификации к которому следует обратиться (если развернуто несколько центров сертификации).

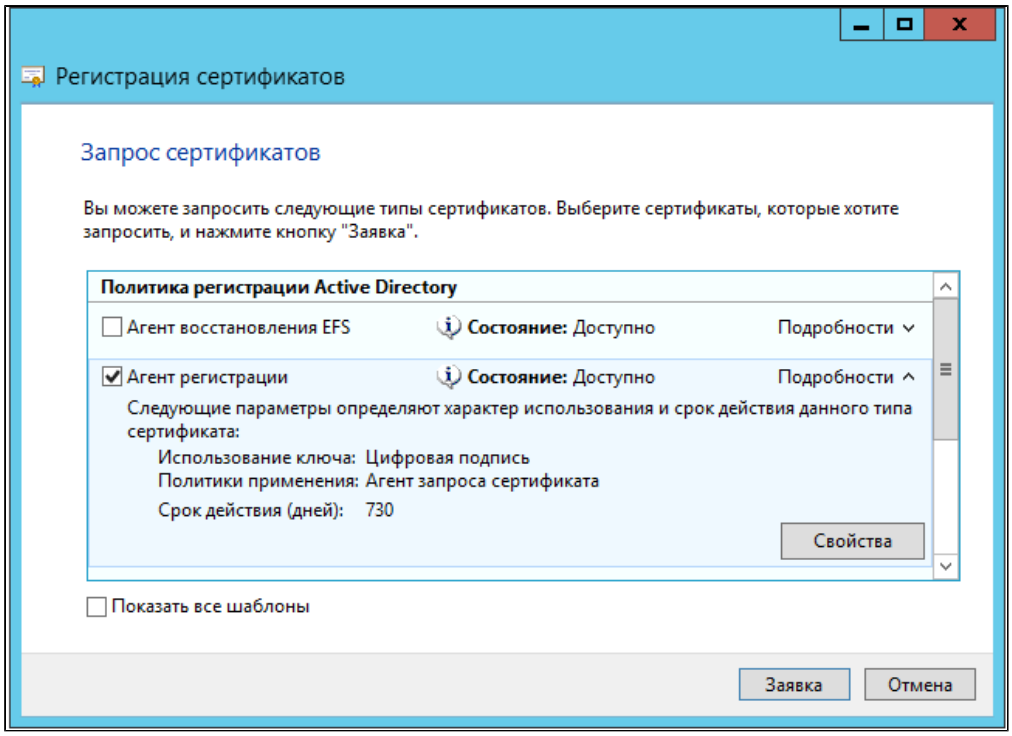
Пример:

KeyBox.CertEnroll.exe /e serviceCA password1 /t=CopyEnrollmentAgent /c=KeyBoxSrv.test.local\test-KeyBoxSrv-CA

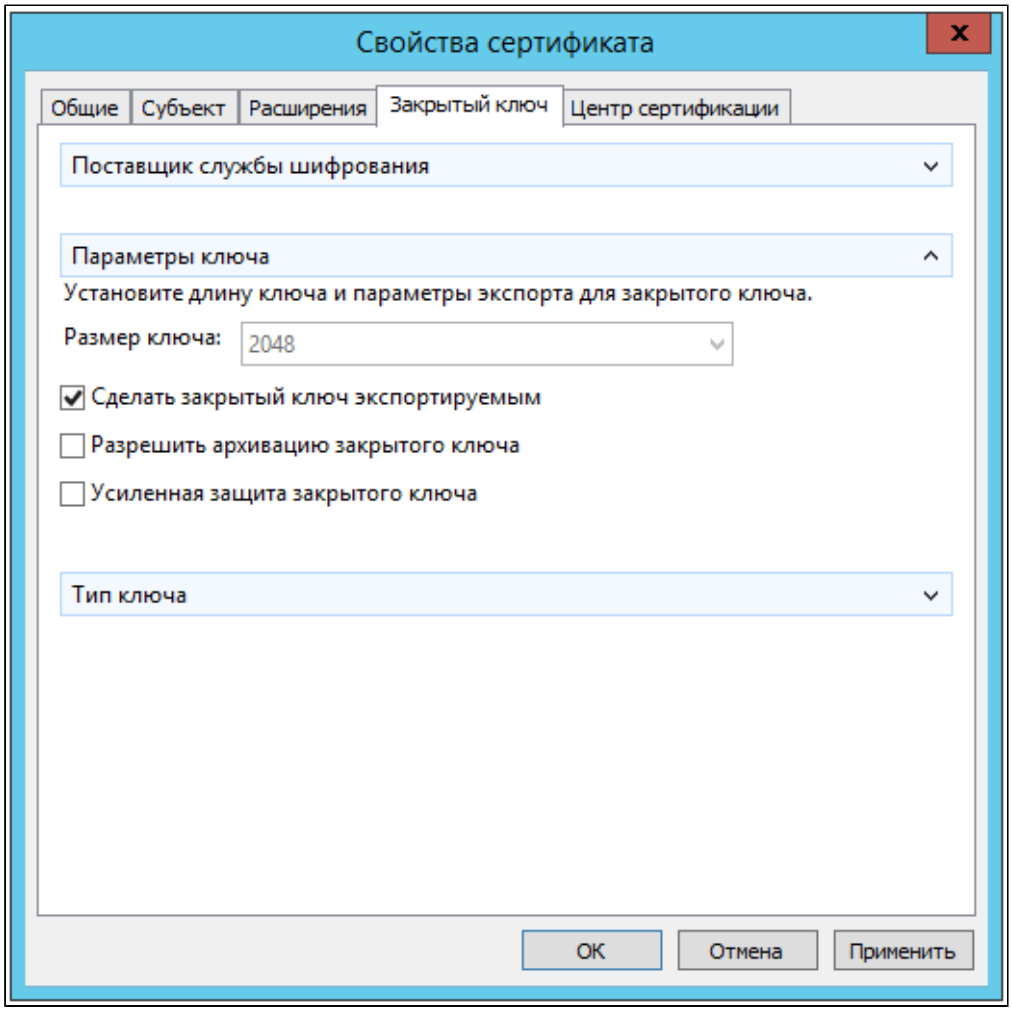
Выпуск сертификата при помощи оснастки Сертификаты (Certificates)

Для выпуска сертификата при помощи оснастки Сертификаты:

1. Выполните вход в систему под сервисной учетной записью (“serviceCA”) и откройте оснастку **Сертифкаты** (Certificates) пользователя.
2. Запустите мастер выпуска нового сертификата.
3. Выберите тип сертификата **Агент регистрации** (Enrollment Agent), разверните окно подробной информации и нажмите кнопку **Свойства** (Properties).



4. Перейдите на вкладку **Закрытый ключ** (Private key), разверните меню **Параметры ключа** (Key options) и включите опцию **Сделать закрытый ключ экспортируемым** (Allow private key to be exported).



5. Переместите выпущенный сертификат и его закрытый ключ в хранилище сертификатов компьютера, на котором развернут сервер Рутокен KeyBox.

6. Выдайте сервисному пользователю (“serviceCA”) права на чтение закрытого ключа сертификата **Агент регистрации** (Enrollment Agent). Для этого в оснастке **Сертификаты** (Certificates) кликните правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) – **Управление закрытыми ключами...** (Manage Private Keys...), нажмите **Добавить** (Add), укажите нужную учетную запись и выставите право **Полный доступ** (Full control). Нажмите **Применить** (Apply).

Таким образом, Вы создали хранилище данных системы **Рутокен KeyBox** в **Active Directory** и произвели необходимые настройки Удостоверяющего Центра Microsoft.

Если Вы планируете использовать помимо удостоверяющего центра Microsoft удостоверяющие центры КриптоПро 1.5 или 2.0, то перейдите к разделам **Настройка системы для использования с удостоверяющим центром Крипто Про 1.5** или **Настройка системы для использования с удостоверяющим центром Крипто Про 2.0** соответственно.

Если использование других удостоверяющих центров не предполагается, то перейдите к разделу **Генерации ключа шифрования**.

Настройка системы для использования с удостоверяющим центром КриптоПро 1.5

Создание сервисных учетных записей для работы с хранилищем данных

Для полноценной работы системы **Рутокен KeyBox** необходимо наличие определенных прав доступа к объектам **Active Directory** и **Центрам сертификации**. В соответствии с принятой в вашей компании политикой безопасности, Вы можете распределить привилегии между несколькими сервисными учетными записями, либо создать сервисную учетную запись с максимальным набором прав на управление системой.

При распределении привилегий, необходимо создать учетные записи.

Учетная запись пользователя (например, **serviceKeyBox**) для работы с контейнером **KeyBox**, от имени которой будут выполняться операции сохранения данных в **Active Directory**. Выдайте данной учетной записи следующие полномочия: полные права (Full Control) на контейнер **KeyBox** и все его дочерние объекты.

Учетная запись пользователя (например, **serviceAD**), от имени которой система будет читать и вносить изменения в профили учетных записей пользователей. Выдайте данной учетной записи следующие полномочия: права на чтение всех свойств пользователей, а также права на запись атрибута **userAccountControl** пользователям.

Для этого выполните следующие действия:

1. Откройте свойство **Безопасность** (Security) контейнера, в котором содержатся пользователи системы Рутокен KeyBox.
2. Нажмите **Добавить** (Add) и качестве пользователя укажите сервисную учетную запись.
3. Нажмите **Дополнительно** (Advanced), выберите сервисную учетную запись и нажмите **Изменить** (Edit).
4. Выберите область применения **Дочерние объекты: Пользователь** (Descendant User objects).
5. Перейдите на вкладку **Свойства** (Properties).
6. Выберите область применения **Дочерние объекты: Пользователь** (Descendant User objects).
7. Поставьте разрешение напротив **Прочитать все свойства** (Read all properties).
8. Поставьте разрешения для пунктов: **Запись: userAccountControl** (Write: userAccountControl).
9. Нажмите **ОК** и затем **Применить** (Apply).

Важная информация

Наличие данной сервисной учетной записи необходимо, только в том случае, если Вы планируете вносить изменения в профиль пользователя **Active Directory** посредством системы Рутокен KeyBox (использование опции "Требовать логон по смарт-карте" в разделе Настройки PKI).

Если пользователи размещены в нескольких контейнерах или подразделениях домена, необходимо для всех контейнеров/подразделений установить одинаковые права для сервисной учетной записи.

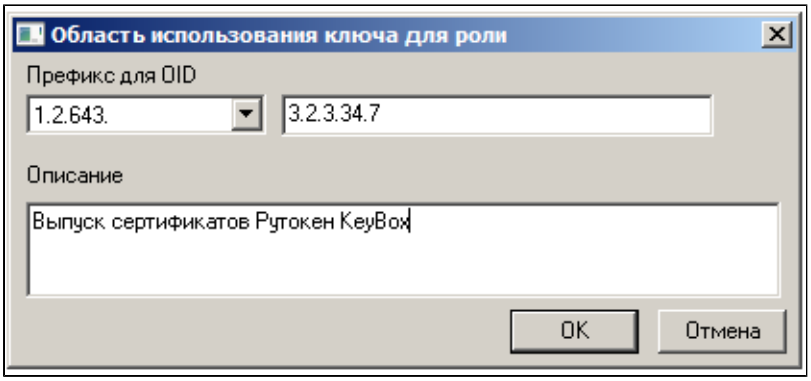
Создание привилегированной роли «Выпуск сертификатов Рутокен KeyBox»

Для создания привилегированной роли "Выпуск сертификатов Рутокен KeyBox":

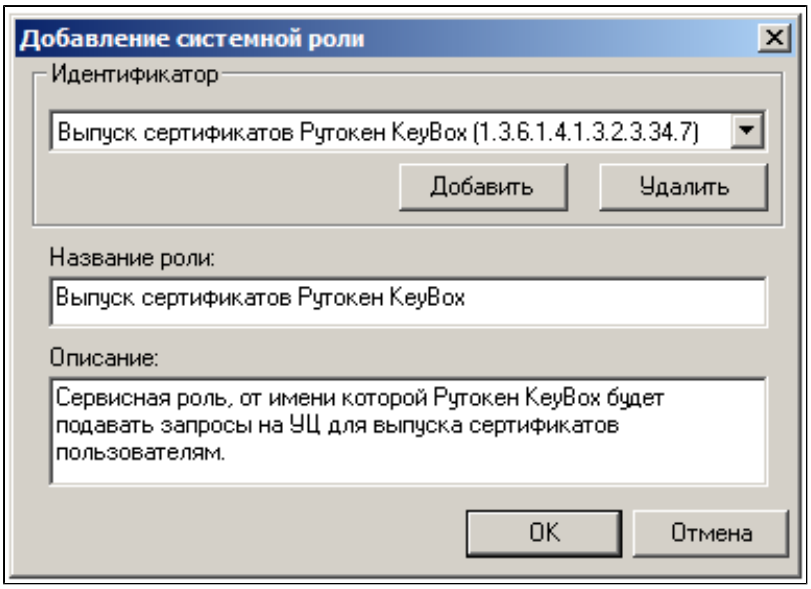
- Откройте приложение **КриптоПро УЦ Центр Регистрации**, перейдите в **Параметры Центра Регистрации**, выберите в списке необходимый Центр Регистрации и перейдите на вкладку **Политики** в его свойствах.
- Откройте **Системные роли** и добавьте новый идентификатор (OID) и его описание.

Важная информация

Для добавления областей использования ключа в системе ЭДО конкретной организации необходимо использовать OIDы, присваиваемые на основе корневого OID организации, полученного официальным путем.



- Перезапустите приложение **КриптоПро УЦ Центр Регистрации** для применения внесенных изменений, перейдите на вкладку **Политики** в свойствах вашего Центра Регистрации и откройте редактор **Системных ролей**.
- Добавьте новую роль **Выпуск сертификатов Рутокен KeyBox** и свяжите его с ранее созданным идентификатором:



- На вкладке **Политики** выберите **Шаблоны сертификатов** и добавьте новый шаблон **Выпуск сертификатов Рутокен KeyBox**, включив следующие области использования ключа:
  - Выпуск сертификатов Рутокен KeyBox
  - Пользователь Центра Регистрации
  - Проверка подлинности клиента
- На вкладке **Политики** для роли **Выпуск сертификатов Рутокен KeyBox** выдайте следующие разрешения и настройте список допустимых использований сертификатов:
  - Обработка запросов на отзыв (улучшенный ключ)
  - Обработка неподписанных запросов (расширения)
  - Обработка неподписанных запросов (улучшенный ключ)
  - Обработка подписанных запросов (расширения)
  - Обработка подписанных запросов (улучшенный ключ)

Важная информация

Списки допустимых использований сертификатов всех разрешений для роли **Выпуск сертификатов Рутокен KeyBox** аналогичны спискам использований сертификатов для роли **Оператор**.

- На вкладке **Безопасность** необходимо добавить следующие разрешения для роли **Выпуск сертификатов Рутокен KeyBox** (действия **Выполнение** и **Делегация**):
  - Получить шаблоны сертификатов (Admin.GetCertTemplates)
  - Получить ограничения на имена DN (Admin.GetGrantedNameProperties)
  - Отправить запрос на публикацию COC (Admin.PublishCRL)
  - Одобрить выпуск сертификата по подписанному запросу на сертификат (CertRequest. AcceptRequest)
  - Одобрить выпуск сертификата по неподписанному запросу на сертификат (CertRequest. AcceptFirstRequest)
  - Подтвердить получение сертификата (CertRequest.ConfirmRequest)

- Отклонить выпуск сертификата по запросу (CertRequest.DenyRequest)
- Получить информацию о сертификате по коду запроса на сертификат (CertRequest.GetCertificateInfo)
- Получить свойства запроса на сертификат (CertRequest.GetRequestInfo)
- Получить список запросов на сертификат (CertRequest.GetRequestsList)
- Отправить неподписанный запрос на сертификат (CertRequest.SubmitFirstCertRequest)
- Отправить подписанный запрос на сертификат (CertRequest.SubmitRequest)
- Получить сертификат Центра Сертификации (CertView.GetCACertificate)
- Получить список сертификатов (CertView.GetCertificatesList)
- Получить информацию о пользователе (UserView.GetUserInfo)
- Получить список отозванных сертификатов (COC) (CertView.GetCRL)
- Одобрить создание пользователя по запросу на регистрацию (Registration.AcceptRequest)
- Отправить запрос на регистрацию пользователя администратором (Registration.CreateRequestByAdmin)
- Одобрить запрос на отзыв сертификата (RevokeRequest.AcceptRevRequest)
- Отправить запрос на отзыв сертификата (RevokeRequest.SubmitRequest)
- Отправить запрос на приостановление действия сертификата (RevokeRequest.SubmitHoldRequest)
- Отправить запрос на возобновление действия сертификата (RevokeRequest.SubmitUnHoldRequest)
- Получить список пользователей (UserView.GetUsersList)
- Одобрить запрос на приостановление сертификата (RevokeRequest.AcceptHoldRequest)
- Одобрить запрос на возобновление сертификата (RevokeRequest.AcceptUnholdRequest)

- Откройте **Центр сертификации** (Certification Authority) и перейдите на вкладку **Модуль политики** (Policy Module) в свойствах центра сертификации КриптоПро.
- Нажмите **Свойства**… (Properties…) и перейдите на вкладку **Использование ключа**
- Добавьте новый идентификатор области использования ключа **Выпуск сертификатов Рутокен KeyBox** в список. Для этого добавьте ранее созданный идентификатор **Выпуск сертификатов Рутокен KeyBox** в список и нажмите кнопку **ОК** и затем **Применить**. Перезапустите центр сертификации.
- Убедитесь в том, что пользователю, подключенному к Центру Регистрации, разрешено выпускать сертификат роли **Выпуск сертификатов Рутокен KeyBox** (соответствующие разрешения должны быть определены в свойствах **Центр Регистрации**- **Политики** – **Обработка не подписанных запросов** (улучшенный ключ)).
- Создайте нового пользователя (например, serviceCA) в Центре Регистрации УЦ КриптоПро и выпустите для него сертификат **Выпуск сертификатов Рутокен KeyBox** с созданием контейнера закрытого ключа на смарт-карте и помещением сертификата в контейнер закрытого ключа (Опция «Установить сертификат в контейнер закрытого ключа»).

Важная информация

Если в дальнейшем предполагается использовать несколько серверов Рутокен KeyBox с общим хранилищем данных совместно с КриптоПро УЦ, то сертификат сервисного пользователя **Выпуск сертификатов Рутокен KeyBox** должен быть выпущен с экспортируемым закрытым ключом. Этот сертификат и его контейнер закрытого ключа необходимо будет переносить на каждый сервер Рутокен KeyBox.

- Установите в хранилище компьютера (Local Computer), на котором установлен сервер Рутокен KeyBox в список **Доверенных Корневых Центров Сертификации** (Trusted Root Certification Authorities) сертификат коревого удостоверяющего центра КриптоПро.
- Установите список отозванных сертификатов удостоверяющего центра КриптоПро в хранилище компьютера (Local Computer), на котором установлен сервер Рутокен KeyBox в **Промежуточные Центры Сертификации** (Intermediate Certification Authorities).
- Запустите на сервере Рутокен KeyBox с правами администратора приложение **КриптоПро CSP** и на вкладке **Сервис** в разделе **Контейнер закрытого ключа** выберите **Скопировать…**
- Подключите смарт-карту, содержащую контейнер закрытого ключа и сертификат, выданный пользователю serviceCA к серверу Рутокен KeyBox и укажите имя ключевого контейнера используя кнопку **Обзор**.
- Укажите, что введённое имя задает ключевой контейнер Пользователя и нажмите **Далее**.
- Задайте уникальное имя создаваемого контейнера и укажите, что оно задает ключевой контейнер Компьютера.
- Завершите копирование, указав хранилище для контейнера закрытого ключа. Рекомендуется использовать тип **«Реестр»**.

Важная информация

Если на сервере Рутокен KeyBox установлен КриптоПро CSP с уровнем безопасности КС1, то во избежание ошибок в работе КриптоПро CSP задавать PIN-код для скопированного контейнера закрытого ключа не нужно.

- Установите в хранилище сертификатов компьютера на сервере Рутокен KeyBox сертификат привилегированной роли КриптоПро (пользователь «serviceCA»). Для этого запустите КриптоПро CSP с правами администратора, перейдите на вкладку **Сервис** в раздел **Сертификаты в контейнере закрытого ключа.** Нажмите **Просмотреть сертификаты в контейнере**, укажите ключевой контейнер Компьютера и укажите имя контейнера используя кнопку **Обзор**. Нажмите кнопку **Далее** и затем **Установить**. Убедитесь, что сертификат появился в хранилище личных сертификатах компьютера.
- Выдайте системе Рутокен KeyBox права на чтение закрытого ключа сертификата привилегированной роли КриптоПро (пользователь «serviceCA»). Для этого в оснастке **Сертификаты** (Certificates) компьютера, на котором установлен сервер Рутокен KeyBox кликните правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) – **Управление закрытыми ключами...** (Manage Private Keys...), нажмите **Добавить** (Add), укажите локальную группу **IIS_IUSRS** (если используется IIS 7.0) или локальную учетную запись **IIS AppPool\Rutoken KeyBox** (если используется IIS 7.5 и более поздние версии) и выставите право **Полный доступ** (Full Control). Нажмите **Применить** (Apply).

Важная информация

Приведенный в пунктах 12-20 способ создания сервисного пользователя и его сертификата не является единственным возможным. Вы можете создать пользователя и запросить сертификат его при помощи web-сервиса КриптоПро УЦ 1.5. Установка в хранилище выполняется средствами КриптоПро CSP.

Таким образом, Вы создали хранилище данных системы Рутокен KeyBox в Active Directory и произвели необходимые настройки Удостоверяющего Центра КриптоПро 1.5.

Если Вы планируете использовать помимо УЦ КриптоПро 1.5 удостоверяющие центры Microsoft или КриптоПро 2.0, то перейдите к разделам **Настройка системы для использования с Удостоверяющего Центра Microsoft** или **Настройка системы для использования с Удостоверяющего Центра Крипто Про 2.0** соответственно.

Если использование других удостоверяющих центров не предполагается, то перейдите к **Генерации ключа шифрования**.

Настройка системы для использования с удостоверяющим центром КриптоПро 2.0

Создание сервисных учетных записей для работы с хранилищем данных

Для полноценной работы системы **Рутокен KeyBox** необходимо наличие определенных прав доступа к объектам **Active Directory** и **Центрам сертификации**. В соответствии с принятой в вашей компании политикой безопасности, Вы можете распределить привилегии между несколькими сервисными учетными записями, либо создать сервисную учетную запись с максимальным набором прав на управление системой.

При распределении привилегий, необходимо создать следующие учетные записи:

- Учетная запись пользователя (например, **serviceKeyBox**) для работы с контейнером **KeyBox**, от имени которой будут выполняться операции сохранения данных в **Active Directory**.
  Выдайте данной учетной записи следующие полномочия:
  - Полные права (Full Control) на контейнер **KeyBox** и все его дочерние объекты.
- Учетная запись пользователя (например, **serviceAD**), от имени которой система будет читать и вносить изменения в профили учетных записей пользователей.
  Выдайте данной учетной записи следующие полномочия:
  - Права на чтение всех свойств пользователей, а также права на запись атрибута **userAccountControl** пользователям.
    Для этого выполните следующие действия:
    - Откройте свойство **Безопасность** (Security) контейнера, в котором содержатся пользователи системы Рутокен KeyBox.
    - Нажмите **Добавить** (Add) и качестве пользователя укажите сервисную учетную запись.
    - Нажмите **Дополнительно** (Advanced), выберите сервисную учетную запись и нажмите **Изменить** (Edit).
    - Выберите область применения **Дочерние объекты: Пользователь** (Descendant User objects).
    - Перейдите на вкладку **Свойства** (Properties).

- Выберите область применения **Дочерние объекты: Пользователь** (Descendant User objects).
- Поставьте разрешение напротив **Прочитать все свойства** (Read all properties).
- Поставьте разрешения для пунктов:
  - **Запись: userAccountControl** (Write: userAccountControl)
- Нажмите **ОК** и затем **Применить** (Apply).

Важная информация

Наличие данной сервисной учетной записи необходимо, только в том случае, если Вы планируете вносить изменения в профиль пользователя **Active Directory** посредством системы Рутокен KeyBox (использование опции "Требовать логон по смарт-карте" в разделе Настройки PKI).

Если пользователи размещены в нескольких контейнерах или подразделениях домена, необходимо для всех контейнеров/подразделений установить одинаковые права для сервисной учетной записи.

Создание сервисной группы пользователей в Центре Регистрации КриптоПро

Для взаимодействия системы Рутокен KeyBox с КриптоПро УЦ 2.0 необходимо наличие сервисной учетной записи, от имени которой Рутокен KeyBox будет обращаться к УЦ для запроса сертификатов пользователей. Вы можете использовать любую имеющуюся в Центре Регистрации учетную запись в качестве сервисной, поместив ее в предварительно созданную и наделенную необходимыми полномочиями сервисную группу системы Рутокен KeyBox. Для создания такой группы и сервисной учетной записи выполните следующие действия:

- Создайте группу безопасности с произвольным именем, например, **KeyBox Service Users** в **Консоли управления ЦР**.
- Откройте свойства папки, в которой будут располагаться пользователи системы **Рутокен KeyBox**, и перейдите на вкладку **Безопасность**.
- Добавьте созданную группу **KeyBox Service Users**.
- Выдайте группе **KeyBox Service Users** следующие разрешения:

Разрешения: Папок

- Чтение свойств
- Запись свойств
- Запрос регистрации
- Одобрение регистрации

Разрешения: Пользователей

- Чтение свойств
- Запрос сертификата
- Запрос аннулирования
- Запрос приостановления
- Запрос возобновления
- Одобрение сертификата

- Одобрение аннулирования
- Одобрение приостановления
- Одобрение возобновления
- Разрешения: Шаблонов
- Запрос сертификата
- Одобрение сертификата
- Откройте **Свойства** папки Центр Регистрации перейдите на вкладку **Безопасность** и выдайте группе **KeyBox Service Users** следующие разрешения:

Разрешения: Папок

- Чтение свойств (необходимо для поиска и отображения пользователей Центра Регистрации в web-сервисах **Рутокен KeyBox**)
- Запись свойств (необходимо для публикации списков отозванных сертификатов системой **Рутокен KeyBox**)

Создание сервисной учетной записи

Важная информация

Описанный ниже вариант создания сервисной учетной записи является рекомендуемым, но не единственным. Вы можете создать учетную запись пользователя и выпустить сертификат непосредственно в Центре Регистрации и затем экспортировать его для установки на сервер Рутокен KeyBox.

- В браузере Internet Explorer на сервере Рутокен KeyBox откройте корневую страницу КриптоПро УЦ 2.0 (https://<имя сервера УЦ>/UI/).
- Подайте заявку на регистрацию сервисной учетной записи:
  - Укажите в заявке имя сервисной учетной записи и e-mail
  - Запомните или запишите выданный ЦР идентификатор и временный пароль
  - Укажите дополнительную информацию, если необходимо или пропустите этот шаг
  - Завершите регистрацию
- Одобрите запрос на регистрацию нового пользователя в Консоли управления ЦР.
- Добавьте созданного пользователя в группу безопасности **KeyBox Service Users**.

Создание шаблона сертификата для сервисной учетной записи

Для сервисной учетной записи системы **Рутокен KeyBox** необходимо создать шаблон сертификата, на основе которого в последствии будет выпущен сертификат.

- Откройте узел **Шаблоны сертификатов** в утилите **Диспетчер УЦ**.
- Создайте шаблон сертификата **KeyBox Service User** на основе шаблона **Пользователь**:
  - Укажите срок действия сертификата
  - На вкладке **Создание ключа** включите опцию **Ключ компьютера (LOCAL_MACHINE)**
  - На вкладке **Расширения** в разделе **Расширенное использование ключа** поставьте отметку напротив пункта **Агент запроса сертификата**.
- Примените изменения.

- Щелкните правой кнопкой мыши по корневому узлу **Роли УЦ** и нажмите кнопку **Обновить.**

Выпуск сертификата агента подачи заявок сервисной учетной записи

- С рабочей станции, на которой установлен сервер **Рутокен KeyBox,** выполните вход в личный кабинет пользователя КриптоПро УЦ по идентификатору и временному паролю сервисной учетной записи.
- Создайте запрос на сертификат, указав шаблон **KeyBox Service User**, криптопровайдер **Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider**.
- Отправьте созданный запрос в **Центр Регистрации**.
- Дождитесь одобрения запроса Оператором Центра Регистрации.
- Перейдите в раздел **Запросы** – **Изготовление** личного кабинета пользователя КриптоПро.
- Загрузите и сохраните изготовленный сертификат.

Важная информация

Если предполагается использовать несколько серверов Рутокен KeyBox с общим хранилищем данных совместно с КриптоПро УЦ, то сертификат сервисного пользователя должен быть выпущен с экспортируемым закрытым ключом. Этот сертификат и его контейнер закрытого ключа необходимо будет переносить на каждый сервер Рутокен KeyBox.

- Установите сертификат в контейнер локального хранилища рабочей станции.
- Выдайте системе Рутокен KeyBox права на чтение закрытого ключа сертификата сервисной учетной записи, который был установлен в п. 7. Для этого в оснастке **Сертификаты** (Certificates) компьютера, на котором установлен сервер Рутокен KeyBox кликните правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) – **Управление закрытыми ключами...** (Manage Private Keys...), нажмите **Добавить** (Add), укажите локальную группу **IIS_IUSRS** (если используется IIS 7.0) или локальную учетную запись **IIS AppPool\Rutoken KeyBox** (если используется IIS 7.5 и более поздние версии) и выставите права **Полный доступ** (Full Control) и **Чтение** (Read). Нажмите **Применить** (Apply).
- Установите в хранилище компьютера (Local computer), на котором установлен сервер Рутокен KeyBox в список **Доверенных Корневых Центров Сертификации** (Trusted Root Certification Authorities) сертификат коревого удостоверяющего центра КриптоПро УЦ 2.0.
- Установите список отозванных сертификатов (CRL) удостоверяющего центра КриптоПро УЦ 2.0 в хранилище компьютера (Local Computer), на котором установлен сервер Рутокен KeyBox в **Промежуточные Центры Сертификации** (Intermediate Certification Authorities).

Хранилище данных расположено в Microsoft SQL, каталог пользователей - в Центре Регистрации КриптоПро УЦ 1.5

Установка серверной части

Установка Рутокен KeyBox Server

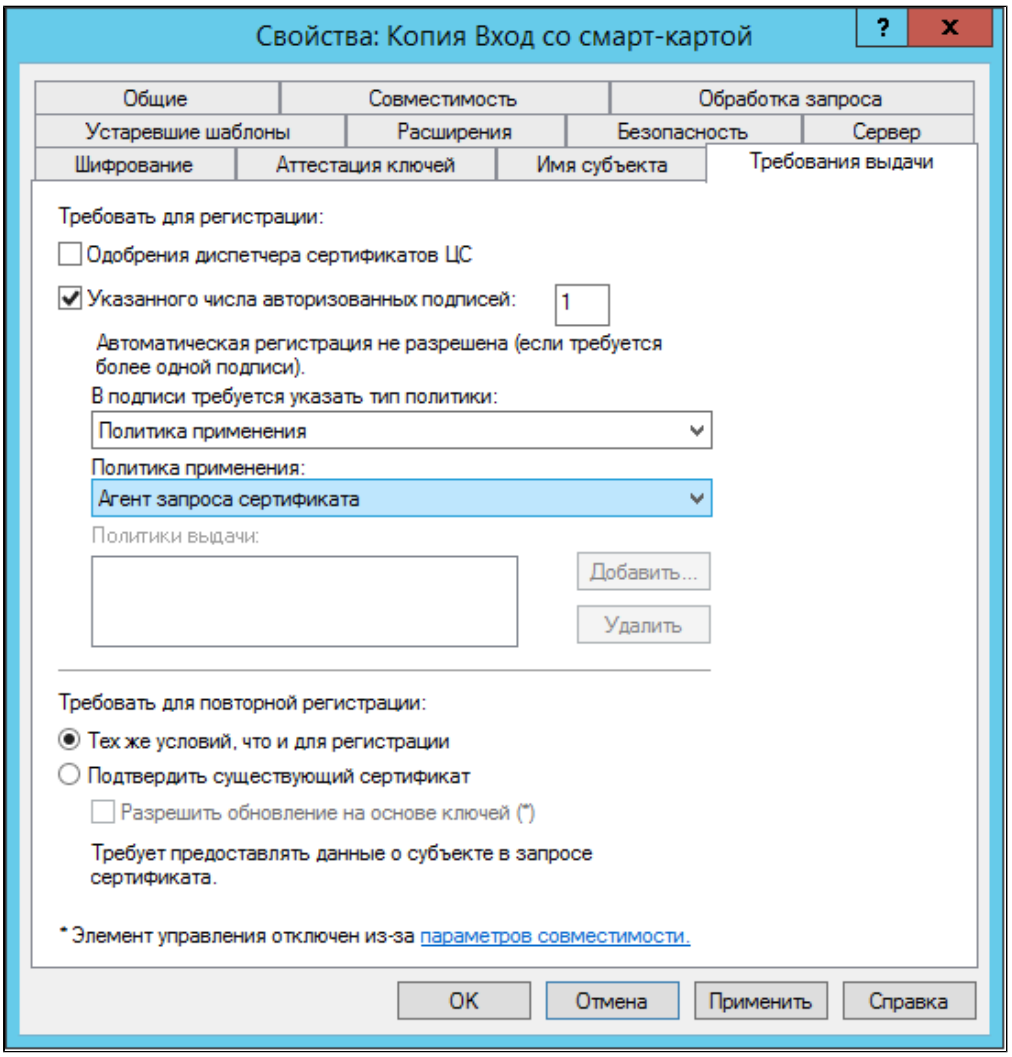
Запустите файл **KeyBox.Server.msi** из дистрибутива Рутокен KeyBox и выполните установку, следуя указаниям мастера.

Создание хранилища в среде Microsoft SQL

Хранилище данных системы Рутокен KeyBox представляет собой базу данных, содержащую набор таблиц для хранения в них всей необходимой информации. База данных создается вручную, а для ее наполнения таблицами используется скрипт **Storage.sql**, входящий в состав дистрибутива Рутокен KeyBox (располагается в KeyBox.Server\Misc\).

Создание базы данных

- Создайте базу данных в среде Microsoft SQL с произвольным именем (например, KeyBox):
  - Определите имя входа (например, KeyBoxSQL)
  - Определите права на работу с базой для создаваемого имени входа, указав следующие разрешения:
    - db_datareader
    - db_datawriter
    - public



Важная информация

Данная учетная запись будет использоваться системой для выполнения операций записи/чтения в базу данных. Имя базы данных, и параметры подключения к ней в дальнейшем будут указаны в файлах конфигурации каждого веб-сервиса системы Рутокен KeyBox.

- Откройте созданную базу данных в среде SQL Management Studio и выполните скрипт **Storage.sql**:
  - Выберите меню **Файл** (File) – **Открыть** (Open) – **Файл…** (File…), укажите путь к файлу **Storage.sql** (располагается в каталоге KeyBox.Server\Misc\) и нажмите **Открыть** (Open).
- Нажмите **Выполнить** (Execute) и после выполнения скрипта обновите содержимое в **Обозревателе объектов** (Object Explorer). Ожидаемый результат – в базе данных KeyBox в разделе **Таблицы** (Tables) появились таблицы:
  - dbo.Cards
  - dbo.CardTypes
  - dbo.Licenses
  - dbo.Policies
  - dbo.Users

Настройка КриптоПро УЦ 1.5

Для работы с УЦ КриптоПро 1.5 потребуется создать несколько ролей:

- Роль **Выпуск сертификатов KeyBox** (для выпуска сертификатов пользователям).
- Роль **Администратор KeyBox** (для создания/изменения/удаления политик, добавления лицензий и типов карт).
- Роль **Оператор KeyBox** (для выпуска и отзыва карт, без возможности изменения конфигурации системы).
- Роль **Пользователь KeyBox** (для доступа к сервису самообслуживания пользователей системы).

Первая роль списка – это своего рода сервисная учетная запись для работы Рутокен KeyBox. Остальные роли предназначены для разграничения доступа внутри системы Рутокен KeyBox (Оператор/Администратор /Пользователь).

Создание системных ролей

Роль «Выпуск сертификатов KeyBox»

- Откройте приложение **КриптоПро УЦ Центр Регистрации**, перейдите в **Параметры Центра Регистрации**, выберите в списке необходимый **Центр Регистрации** и перейдите на вкладку **Политики** в его **Свойствах**.
- Откройте **Системные роли** и добавьте новый идентификатор (**OID**) и его описание.

Важная информация

Для добавления областей использования ключа в системе ЭДО конкретной организации необходимо использовать OID'ы, присваиваемые на основе корневого OID организации, полученного официальным путем.

- Перезапустите приложение **КриптоПро УЦ Центр Регистрации** для применения внесенных изменений, перейдите на вкладку **Политики** в **Свойствах** Центра Регистрации и откройте **Редактор Системных ролей**.
- Добавьте новую роль **Выпуск сертификатов KeyBox** и свяжите её с ранее созданным идентификатором.
- На вкладке **Политики** выберите **Шаблоны сертификатов** и добавьте новый шаблон **Выпуск сертификатов KeyBox**, включив следующие области использования ключа:
  - **Выпуск сертификатов KeyBox**
  - **Пользователь Центра Регистрации**
  - **Проверка подлинности клиента**
- На вкладке **Политики** для роли **Выпуск сертификатов KeyBox** выдайте следующие разрешения и настройте список допустимых использований сертификатов:
  - Обработка запросов на отзыв (улучшенный ключ)
  - Обработка неподписанных запросов (расширения)
  - Обработка неподписанных запросов (улучшенный ключ)
  - Обработка подписанных запросов (расширения)
  - Обработка подписанных запросов (улучшенный ключ)
- На вкладке **Безопасность** необходимо добавить следующие разрешения для роли **Выпуск сертификатов KeyBox** (действия **Выполнение** и **Делегация**):
  - Получить шаблоны сертификатов (Admin.GetCertTemplates)
  - Получить ограничения на имена DN (Admin.GetGrantedNameProperties)
  - Отправить запрос на публикацию COC (Admin.PublishCRL)
  - Одобрить выпуск сертификата по подписанному запросу на сертификат (CertRequest. AcceptRequest)
  - Одобрить выпуск сертификата по неподписанному запросу на сертификат (CertRequest. AcceptFirstRequest)
  - Подтвердить получение сертификата (CertRequest.ConfirmRequest)
  - Отклонить выпуск сертификата по запросу (CertRequest.DenyRequest)
  - Получить информацию о сертификате по коду запроса на сертификат (CertRequest. GetCertificateInfo)
  - Получить свойства запроса на сертификат (CertRequest.GetRequestInfo)
  - Получить список запросов на сертификат (CertRequest.GetRequestsList)
  - Отправить неподписанный запрос на сертификат (CertRequest.SubmitFirstCertRequest)
  - Отправить подписанный запрос на сертификат (CertRequest.SubmitRequest)
  - Получить сертификат Центра Сертификации (CertView.GetCACertificate)
  - Получить список сертификатов (CertView.GetCertificatesList)
  - Получить информацию о пользователе (UserView.GetUserInfo)
  - Получить список отозванных сертификатов (COC) (CertView.GetCRL)
  - Одобрить создание пользователя по запросу на регистрацию (Registration.AcceptRequest)
  - Отправить запрос на регистрацию пользователя администратором (Registration. CreateRequestByAdmin)

- Одобрить запрос на отзыв сертификата (RevokeRequest.AcceptRevRequest)
- Отправить запрос на отзыв сертификата (RevokeRequest.SubmitRequest)
- Отправить запрос на приостановление действия сертификата (RevokeRequest.SubmitHoldRequest)
- Отправить запрос на возобновление действия сертификата (RevokeRequest.SubmitUnHoldRequest)
- Получить список пользователей (UserView.GetUsersList)
- Одобрить запрос на приостановление сертификата (RevokeRequest.AcceptHoldRequest)
- Одобрить запрос на возобновление сертификата (RevokeRequest.AcceptUnholdRequest)
- Нажмите **Применить**.

- Откройте оснастку **Центр сертификации** и перейдите на вкладку **Модуль политики** в **Свойствах** Центра Сертификации КриптоПро.
- Нажмите **Свойства**… и перейдите на вкладку **Использование ключа**
- Добавьте новый идентификатор области использования ключа **Выпуск сертификатов KeyBox** в список. Перезапустите Центр Сертификации КриптоПро.
- Создайте нового пользователя (например, **KeyBox Enrollment Agent**) в **АРМ Администратора КриптоПро** и выпустите для него сертификат **Выпуск сертификатов KeyBox** с созданием контейнера закрытого ключа на смарт-карте и помещением сертификата в контейнер закрытого ключа (Опция **Установить сертификат в контейнер закрытого ключа**).

Важная информация

Если в дальнейшем предполагается использовать несколько серверов Рутокен KeyBox с общим хранилищем данных совместно с КриптоПро УЦ, то сертификат сервисного пользователя Администратор KeyBox должен быть выпущен с экспортируемым закрытым ключом. Этот сертификат и его контейнер закрытого ключа необходимо будет переносить на каждый сервер Рутокен KeyBox.

- Установите в хранилище компьютера (Local computer), на котором установлен сервер Рутокен KeyBox в список **Доверенных Корневых Центров Сертификации** (Trusted Root Certification Authorities) сертификат Удостоверяющего Центра КриптоПро.
- Установите список отозванных сертификатов Удостоверяющего Центра КриптоПро в хранилище компьютера (Local Computer), на котором установлен сервер Рутокен KeyBox в **Промежуточные Центры Сертификации** (Intermediate Certification Authorities).
- Запустите на сервере Рутокен KeyBox с правами администратора приложение **КриптоПро CSP** и на вкладке **Сервис** в разделе **Контейнер закрытого ключа** выберите **Скопировать**…
- Подключите смарт-карту, содержащую контейнер закрытого ключа и сертификат, выданный пользователю **KeyBox Enrollment Agent** к серверу Рутокен KeyBox и укажите имя ключевого контейнера используя кнопку **Обзор**.
- Укажите, что введённое имя задает ключевой контейнер **Пользователя** и нажмите **Далее**.
- Задайте уникальное имя создаваемого контейнера и укажите, что оно задает ключевой контейнер **Компьютера**. Завершите копирование, указав хранилище для контейнера закрытого ключа. Рекомендуется использовать тип **Реестр**.

Важная информация

Если на сервере Рутокен KeyBox установлен КриптоПро CSP с уровнем безопасности КС1, то задавать PIN-код для скопированного контейнера закрытого ключа не нужно.

- Установите в хранилище сертификатов компьютера на сервере Рутокен KeyBox сертификат привилегированной роли КриптоПро (пользователь **KeyBox Enrollment Agent**). Для этого запустите **КриптоПро CSP** с правами администратора, перейдите на вкладку **Сервис** в раздел **Сертификаты в контейнере закрытого ключа**. Нажмите **Просмотреть сертификаты в контейнере**, укажите ключевой контейнер **Компьютера** и укажите имя контейнера (созданного ранее) используя кнопку **Обзор**. Нажмите **Далее** и затем **Установить**. Убедитесь в том, что сертификат появился в хранилище личных сертификатах компьютера.
- Выдайте системе Рутокен KeyBox права на чтение закрытого ключа сертификата привилегированной роли КриптоПро (пользователь **KeyBox Enrollment Agent**). Для этого в оснастке **Сертификаты** (Certificates) компьютера, на котором установлен сервер Рутокен KeyBox кликните правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) – **Управление закрытыми ключами...** (Manage Private Keys...), нажмите **Добавить** (Add), укажите локальную группу **IIS_IUSRS** (если используется IIS 7.0) или локальную учетную запись **IIS AppPool\KeyBox** (если используется IIS 7.5 и более поздние версии) и выставите права **Полный доступ** (Full Control) и **Чтение** (Read). Нажмите **Применить** (Apply).

Ожидаемый результат:

- В КриптоПро УЦ создана роль **Выпуск сертификатов KeyBox**, в **АРМ Администратора Центра Регистрации КриптоПро** создан пользователь **KeyBox Enrollment Agent**, которому выпущен сертификат роли **Выпуск сертификатов KeyBox**.
- На сервере Рутокен KeyBox в хранилище компьютера находится сертификаты:
  - Корневого УЦ КриптоПро в разделах **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities), **Промежуточные центры сертификации - Список отзыва сертификатов** (Intermediate Certification Authorities – Certificate Revocation List)
  - Пользователя **KeyBox Enrollment Agent** с выставленным разрешением на управление его закрытым ключом для групп **IIS_IUSRS** или **IIS AppPool\KeyBox**
- В хранилище **Реестр** рабочей станции с установленным сервером Рутокен KeyBox создан контейнер, в котором хранится закрытый ключ сертификата роли **Выпуск сертификатов KeyBox**, выданного пользователю **KeyBox Enrollment Agent**.

Роли "Администратор KeyBox" и "Оператор KeyBox"

Аутентификация пользователей в web-сервисах системы **Рутокен KeyBox** в рассматриваемой конфигурации будет осуществляться по их персональным сертификатам. Для того, чтобы различать обычных пользователей и пользователей-администраторов (операторов) необходимо создать соответствующие роли в КриптоПро УЦ. Для каждой роли будет создан шаблон сертификата, включающий в себя уникальное значение **Улучшенного ключа** (EKU, Extended Key Usage). На основе этого значения (указанного в файлах конфигурации каждого web-приложения для каждой группы пользователей) **Рутокен KeyBox** будет определять к какой из групп принадлежит пользователь, предоставивший свой сертификат для получения доступа к тому или иному web-сервису **Рутокен KeyBox**.

Важная информация

Аутентификация может осуществляться не только по значению расширенного использования ключа (EKU), но и по уникальному отпечатку (Thumbprint) сертификата. Подробнее о настройке аутентификации в файлах конфигурации см. в разделе Конфигурирование Management Console.

Роли **Администратор KeyBox** и **Оператор KeyBox** создаются по аналогии с ролью **Выпуск сертификатов KeyBox**. Затем выполните следующие операции:

- Добавьте новую роль **Администратор KeyBox** (**Оператор KeyBox**) и свяжите её с ранее созданным идентификатором:
  - На вкладке **Политики** выберите **Шаблоны сертификатов** и добавьте новый шаблон **Администратор KeyBox** (**Оператор KeyBox**), включив следующие области использования ключа:
    - Пользователь Центра Регистрации
- Выполните создание идентификатора области использования ключа для роли **Администратор KeyBox** (**Оператор KeyBox**) по аналогии с созданием роли **Выпуск сертификатов KeyBox**
- Создайте новых пользователей (например, **Администратор KeyBox** и **Оператор KeyBox**) в **АРМ Администратора КриптоПро** и выпустите для них сертификаты **Администратор KeyBox** и **Оператор KeyBox** соответственно с созданием контейнера закрытого ключа на смарт-карте и помещением сертификата в контейнер закрытого ключа (Опция **Установить сертификат в контейнер закрытого ключа**).

Используя сертификат с закрытым ключом на смарт-карте, сотрудник, наделенный ролью **Администратор KeyBox** (**Оператор KeyBox**) сможет попасть в сервис **Консоль управления Рутокен KeyBox** только с использованием данной смарт-карты.

Роль «Пользователь KeyBox»

По аналогии с ролями "**Администратор KeyBox**" и "**Оператор KeyBox**" можно создать и привилегированную роль "**Пользователь KeyBox**". В этом случае доступ к сервису самообслуживания (Self Service) смогут получать только пользователи, обладающие сертификатом этой роли.

Однако, наличие такой роли не обязательно – можно считать пользователями **Рутокен KeyBox** всех пользователей **Центра Регистрации КриптоПро 1.5**, в сертификатах которых есть значение **1.2.643.2.2.34.6 «Пользователь Центра Регистрации, HTTP, TLS клиент»** в поле **Улучшенный ключ** (Extended Key Usage).

Таким образом, Вы создали хранилище данных системы **Рутокен KeyBox** в **Microsoft SQL** и произвели необходимые настройки удостоверяющего центра КриптоПро 1.5.

Если Вы планируете использовать помимо удостоверяющего центра КриптоПро 1.5 удостоверяющий центр Крипто Про 2.0, то перейдите к разделу **Работа с КриптоПро УЦ 2.0**.

Если использование других удостоверяющих центров не предполагается, то перейдите к **Генерации ключа шифрования**.

Работа с КриптоПро УЦ 2.0

Рутокен KeyBox поддерживает конфигурацию с несколькими удостоверяющими центрами КриптоПро версий 1.5 и 2.0, использующих один каталог пользователей. Добавление КриптоПро УЦ 2.0 в подобную конфигурацию производится по аналогии с настройкой УЦ для работы с каталогом пользователей Active Directory (см. **Настройка системы для использования с УЦ КриптоПро 2.0**).

Хранилище данных расположено в Microsoft SQL, каталог пользователей - в Центре Регистрации КриптоПро УЦ 2.0

Установка серверной части

Установка Рутокен KeyBox Server

Запустите файл **KeyBox.Server.exe** из дистрибутива Рутокен KeyBox и выполните установку, следуя указаниям мастера.

Создание хранилища в среде Microsoft SQL

Хранилище данных системы Рутокен KeyBox представляет собой базу данных, содержащую набор таблиц для хранения в них всей необходимой информации. База данных создается вручную, а для ее наполнения таблицами используется скрипт **Storage.sql**, входящий в состав дистрибутива Рутокен KeyBox (располагается в KeyBox.Server\Misc\).

Создание базы данных

- Создайте базу данных в среде Microsoft SQL с произвольным именем (например, KeyBox):
  - Определите имя входа (например, KeyBoxSQL)
  - Определите права на работу с базой для создаваемого имени входа, указав следующие разрешения:
    - db_datareader
    - db_datawriter
    - public

Важная информация

Данная учетная запись будет использоваться системой для выполнения операций записи/чтения в базу данных. Имя базы данных, и параметры подключения к ней в дальнейшем будут указаны в файлах конфигурации каждого веб-сервиса системы Рутокен KeyBox.

- Откройте созданную базу данных в среде SQL Management Studio и выполните скрипт **Storage.sql**:
  - Выберите меню **Файл** (File) – **Открыть** (Open) – **Файл…** (File…), укажите путь к файлу **Storage.sql** (располагается в каталоге KeyBox.Server\Misc\) и нажмите **Открыть** (Open).
- Нажмите **Выполнить** (Execute) и после выполнения скрипта обновите содержимое в **Обозревателе объектов** (Object Explorer). Ожидаемый результат – в базе данных KeyBox в разделе **Таблицы** (Tables) появились таблицы:

- dbo.Cards
- dbo.CardTypes
- dbo.Licenses
- dbo.Policies
- dbo.Users

Настройка КриптоПро УЦ 2.0

Для взаимодействия системы Рутокен KeyBox с КриптоПро УЦ 2.0 необходимо наличие сервисной учетной записи, от имени которой Рутокен KeyBox будет обращаться к УЦ для запроса сертификатов пользователей. Вы можете использовать любую имеющуюся в Центре Регистрации учетную запись в качестве сервисной, поместив её в предварительно созданную и наделенную необходимыми полномочиями сервисную группу системы Рутокен KeyBox.

Создание сервисной группы пользователей в Центре Регистрации КриптоПро

Для взаимодействия системы Рутокен KeyBox с КриптоПро УЦ 2.0 необходимо наличие сервисной учетной записи, от имени которой Рутокен KeyBox будет обращаться к УЦ для запроса сертификатов пользователей. Вы можете использовать любую имеющуюся в Центре Регистрации учетную запись в качестве сервисной, поместив ее в предварительно созданную и наделенную необходимыми полномочиями сервисную группу системы Рутокен KeyBox. Для создания такой группы и сервисной учетной записи выполните следующие действия:

- Создайте группу безопасности с произвольным именем, например, **KeyBox Service Users** в **Консоли управления ЦР**.
- Откройте свойства папки, в которой будут располагаться пользователи системы Рутокен KeyBox, и перейдите на вкладку **Безопасность**.
- Добавьте созданную группу **KeyBox Service Users**.
- Выдайте группе **KeyBox Service Users** следующие разрешения:

Разрешения: Папок

- Чтение свойств
- Запись свойств
- Запрос регистрации
- Одобрение регистрации

Разрешения: Пользователей

- Чтение свойств
- Запрос сертификата
- Запрос аннулирования
- Запрос приостановления
- Запрос возобновления

- Одобрение сертификата
- Одобрение аннулирования
- Одобрение приостановления
- Одобрение возобновления
- Разрешения: Шаблонов
- Запрос сертификата
- Одобрение сертификата
- Откройте **Свойства** папки Центр Регистрации перейдите на вкладку **Безопасность** и выдайте группе **KeyBox Service Users** следующие разрешения:

Разрешения: Папок

- Чтение свойств (необходимо для поиска и отображения пользователей Центра Регистрации в web-сервисах **Рутокен KeyBox**)
- Запись свойств (необходимо для публикации списков отозванных сертификатов системой **Рутокен KeyBox**)

Создание сервисной учетной записи

Важная информация

Описанный ниже вариант создания сервисной учетной записи является рекомендуемым, но не единственным. Вы можете создать учетную запись пользователя и выпустить сертификат непосредственно в Центре Регистрации и затем экспортировать его для установки на сервер Рутокен KeyBox.

- В браузере Internet Explorer на сервере **Рутокен KeyBox** откройте корневую страницу КриптоПро УЦ 2.0 (https://<имя сервера УЦ>/UI/).
- Подайте заявку на регистрацию сервисной учетной записи:
  - Укажите в заявке имя сервисной учетной записи и e-mail
  - Запомните или запишите выданный ЦР идентификатор и временный пароль
  - Укажите дополнительную информацию, если необходимо или пропустите этот шаг
  - Завершите регистрацию
- Одобрите запрос на регистрацию нового пользователя в Консоли управления ЦР.
- Добавьте созданного пользователя в группу безопасности **“KeyBox Service Users”**.

Создание шаблона сертификата для сервисной учетной записи

Для сервисной учетной записи системы **Рутокен KeyBox** необходимо создать шаблон сертификата, на основе которого в последствии будет выпущен сертификат.

- Откройте узел **Шаблоны сертификатов** в утилите **Диспетчер УЦ**.
- Создайте шаблон сертификата **KeyBox Service User** на основе шаблона **Пользователь**:
  - Укажите срок действия сертификата

- На вкладке **Создание ключа** включите опцию **Ключ компьютера (LOCAL_MACHINE)**
- На вкладке **Расширения** в разделе **Расширенное использование ключа** поставьте отметку напротив пункта **Агент запроса сертификата**.

- Примените изменения.
- Щелкните правой кнопкой мыши по корневому узлу **Роли УЦ** и нажмите кнопку **Обновить**.

Выпуск сертификата агента подачи заявок сервисной учетной записи

- С рабочей станции, на которой установлен сервер Рутокен KeyBox, выполните вход в личный кабинет пользователя КриптоПро УЦ по идентификатору и временному паролю сервисной учетной записи.
- Создайте запрос на сертификат, указав шаблон **KeyBox Service User**, криптопровайдер **Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider**.
- Отправьте созданный запрос в **Центр Регистрации**.
- Дождитесь одобрения запроса Оператором Центра Регистрации.
- Перейдите в раздел **Запросы** – **Изготовление** личного кабинета пользователя КриптоПро.
- Загрузите и сохраните изготовленный сертификат.

Важная информация

Если предполагается использовать несколько серверов Рутокен KeyBox с общим хранилищем данных совместно с КриптоПро УЦ, то сертификат сервисного пользователя должен быть выпущен с экспортируемым закрытым ключом. Этот сертификат и его контейнер закрытого ключа необходимо будет переносить на каждый сервер Рутокен KeyBox.

- Установите сертификат в контейнер локального хранилища рабочей станции.
- Выдайте системе Рутокен KeyBox права на чтение закрытого ключа сертификата сервисной учетной записи. Для этого в оснастке **Сертификаты** (Certificates) компьютера, на котором установлен сервер Рутокен KeyBox кликните правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) – **Управление закрытыми ключами...** (Manage Private Keys...), нажмите **Добавить** (Add), укажите локальную группу**IIS_IUSRS** (если используется IIS 7.0) или локальную учетную запись **IIS AppPool\KeyBox** (если используется IIS 7.5 и более поздние версии) и выставите права **Полный доступ** (Full Control) и **Чтение** (Read). Нажмите**Применить** (Apply).
- Установите в хранилище компьютера (Local computer), на котором установлен сервер **Рутокен KeyBox** в список **Доверенных Корневых Центров Сертификации** (Trusted Root Certification Authorities) сертификат коревого удостоверяющего центра КриптоПро УЦ 2.0.
- Установите список отозванных сертификатов (CRL) удостоверяющего центра КриптоПро УЦ 2.0 в хранилище компьютера (Local Computer), на котором установлен сервер Рутокен KeyBox в **Промежуточные Центры Сертификации** (Intermediate Certification Authorities).

Создание шаблонов сертификатов системных ролей

Для работы с УЦ КриптоПро 2.0, выступающем в качестве каталога пользователей системы Рутокен KeyBox, потребуется создать несколько ролей:

- Роль **Администратор KeyBox** (для создания/изменения/удаления политик, добавления лицензий и типов карт).

- Роль **Оператор KeyBox** (для выпуска и отзыва карт, без возможности изменения конфигурации системы).
- Роль **Пользователь KeyBox** (для доступа к сервису самообслуживания пользователей системы).

Для каждой роли будет создан уникальный шаблон сертификата. В зависимости от предоставленного пользователем при входе на web-страницу сервиса Рутокен KeyBox сертификата система определит принадлежность пользователя к той или иной роли. Шаблоны сертификатов для всех ролей создаются на основе шаблона **Пользователь**, однако для определения принадлежности пользователя к той или иной роли будут использоваться **Отпечаток** (Thumbprint) и значение поля **Улучшенный ключ** (Extended Key Usage) предоставленного сертификата.

Шаблоны «Администратор KeyBox» и «Оператор KeyBox»

- Откройте узел **Шаблоны сертификатов** в утилите **Диспетчер УЦ**.
- Создайте шаблон сертификата **Администратор KeyBox** на основе шаблона **Пользователь**:
  - Укажите срок действия сертификата
- Примените изменения.
- Щелкните правой кнопкой мыши по корневому узлу **Роли УЦ** и нажмите кнопку **Обновить**.
- Выпустите сертификат **Администратор KeyBox** пользователю с сохранением его закрытого ключа на смарт-карте.
- Аналогичным образом создайте шаблон **Оператор KeyBox.**

Шаблон «Пользователь KeyBox»

- Откройте узел **Шаблоны сертификатов** в утилите **Диспетчер УЦ**.
- Создайте шаблон сертификата **Пользователь KeyBox** на основе шаблона **Пользователь**:
  - Укажите срок действия сертификата
  - На вкладке **Расширения** в разделе **Расширенное использование ключа** поставьте отметку напротив пункта **Пользователь Центра Регистрации, HTTP, TLS клиент**.
- Примените изменения.
- Щелкнуть правой кнопкой мыши по корневому узлу **Роли УЦ** и нажмите кнопку **Обновить**.

Таким образом, Вы создали хранилище данных системы Рутокен KeyBox в Microsoft SQL и произвели необходимые настройки удостоверяющего центра КриптоПро 2.0.

Если Вы планируете использовать помимо удостоверяющего центра КриптоПро 2.0 удостоверяющий центр Крипто Про 1.5, то перейдите к разделу **Работа с КриптоПро УЦ 1.5.**

Если использование других удостоверяющих центров не предполагается, то перейдите к **Генерации ключа шифрования.**

Работа с КриптоПро УЦ 1.5

Рутокен KeyBox поддерживает конфигурацию с несколькими удостоверяющими центрами КриптоПро версий 2.0 и 1.5, использующих один каталог пользователей. Добавление КриптоПро УЦ 1.5 в подобную конфигурацию производится по аналогии с настройкой УЦ для работы с каталогом пользователей Active Directory (см. **Настройка системы для использования с УЦ КриптоПро 1.5**).

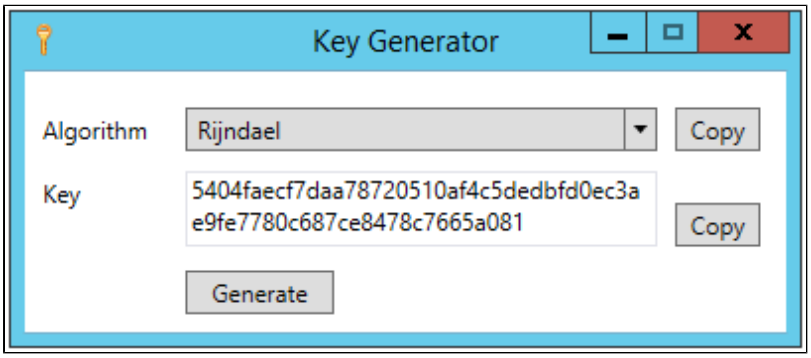
Генерация ключа шифрования

Все данные, с которыми работает система Рутокен KeyBox (политики, лицензии, типы смарт-карт, состояния смарт-карт, данные пользователей и т.д.) хранятся в зашифрованном виде в хранилище данных системы (Active Directory или база данных SQL). Шифрование данных может осуществляться по одному из следующих алгоритмов:

- DES
- TripleDES
- RC2
- Rijndael
- AES

Для генерации ключа шифрования воспользуйтесь утилитой Рутокен KeyBox Key Generator, входящей в состав дистрибутива **Рутокен KeyBox** (располагается в KeyBox.Server\Misc\).

Запустите утилиту **KeyBox.KeyGen.exe**, выберите алгоритм шифрования и нажмите кнопку **Generate**. Чтобы скопировать алгоритм или ключ шифрования в буфер обмена нажмите кнопку **Copy**.



Обязательно сохраните ключ и алгоритм шифрования!

Ключ понадобиться Вам для восстановления системы Рутокен KeyBox в случае поломки сервера либо для развертывания дополнительного сервера Рутокен KeyBox.

Для продолжения настройки системы перейдите к **Настройке файлов конфигурации web-приложений Рутокен KeyBox**.

Настройка файлов конфигурации web-приложений

Система Рутокен KeyBox состоит из набора сервисов (Консоль управления, Сервис самообслуживания, Сервис удаленного самообслуживания, Сервис разблокировки смарт-карт), каждый из которых имеет

свойственные ему файлы конфигурации. На этапе развертывания системы необходимо указать нужные значения в файлах конфигурации для каждого сервиса. Файлы конфигурации всех сервисов системы располагаются в корневом каталоге веб-приложений IIS (путь по умолчанию “%SystemDrive%:\inetpub\wwwroot\”).

Конфигурирование Management Console

Сервис предназначен для настройки системы Рутокен KeyBox, управления смарт-картами и администрирования системы. Файлы конфигурации по умолчанию располагаются в %SystemDrive%:\inetpub\wwwroot\keybox.

Общие параметры для всех конфигураций

Откройте от имени администратора на редактирование файл **keybox\Web.config**. В тэге ***<managementConsoleSettings/>*** содержатся общие для всех конфигураций параметры приложения Management Console.

Названия и описания параметров тега ***<managementConsoleSettings/>***.

Название параметра	**Описание**	**Значение по умолчанию**
cpClientCertificateEKUs	OID системной роли для работы с КриптоПРО УЦ 1.5 (см. Создание привилегированной роли “Выпуск сертификатов Indeed CM". Если Крипто ПРО УЦ 1.5 не используется в вашей конфигурации, то значение следует оставить пустым.	"1.2.643.2.2.34.4" - Администратор Центра Регистрации.
cp2ClientCertificateEKUs	Улучшенный ключ (EKU, Extended Key Usage) сертификата сервисной учетной записи для работы с КриптоПРО УЦ 2.0 (см. Создание шаблона сертификата для сервисной учетной записи). Если КриптоПРО УЦ 2.0 не используется в вашей конфигурации, то значение следует оставить пустым.	"1.3.6.1.5.5.7.3.2" - Проверка подлинности клиента
showMsPkiSettings	Параметр отображения настроек PKI для Microsoft CA. Возможные значения: "true" - отображать, "false" – не отображать.	"true"
showCpPkiSettings	Параметр отображения настроек PKI для Крипто ПРО УЦ 1.5. Возможные значения: "true" - отображать, "false" – не отображать.	"true"
showCp2PkiSettings	Параметр отображения настроек PKI для Крипто ПРО УЦ 2.0. Возможные значения: "true" - отображать, "false" – не отображать.	"false"
showEASettings		"false"

Название параметра	Описание	Значение по умолчанию
	Параметр отображения настроек интеграции с системой Indeed Enterprise Authentication. Возможные значения: "true" - отображать, "false" - не отображать.	
showEnforceSmartCardLogonSetting	Параметр отображения настроек опции «Требовать логон по смарт-карте». Возможные значения: "true" - отображать, "false" - не отображать.	"true"

Важная информация

Учетные данные, содержащиеся в файлах конфигурации рекомендуется зашифровать для повышения уровня безопасности. См. **Шифрование данных в файлах конфигурации web-приложений.**

Параметры для конфигурации, когда хранилище данных и пользователи системы Рутокен KeyBox расположены в Active Directory

После заполнения обязательного тэга ***<managementConsoleSettings/>*** удалите из файла конфигурации следующие строки:

<!--<sqlPersistenceSettings connectionString="CONNECTION_STRING" cryptoAlgName="Rijndael" cryptoKey="CRYPTO_KEY"/>-->

<!--<cpUserCatalogSettings raServiceUrl="RA_SERVICE_URL" clientCertificateThumbprint="CLIENT_CERTIFICATE_THUMBPRINT">-->

<!--<cp2UserCatalogSettings raServiceUrl="RA_SERVICE_URL" clientCertificateThumbprint="CLIENT_CERTIFICATE_THUMBPRINT"/>-->

Строки содержат параметры для подключения к базе данных SQL и каталогам пользователей КриптоПРО УЦ 1.5 и 2.0.

Заполните нижеследующие теги:

- ***<adPersistenceSettings/>*** – параметры подключения к хранилищу данных Рутокен KeyBox
  - ***path*** - путь к хранилищу данных системы, созданному в Active Directory с помощью утилиты KeyBox.StorageAD.exe
  - ***userName*** - имя сервисной учетной записи для работы с хранилищем данных (“serviceKeyBox”)

- ***password*** – пароль для сервисной учетной записи
- ***cryptoAlgName*** – название алгоритма шифрования, который Вы выбрали на этапе генерации ключа шифрования при помощи утилиты KeyBox.KeyGen.exe
- ***cryptoKey*** – ключ шифрования, полученный при помощи утилиты KeyBox.KeyGen.exe

- **<*adUserCatalogSettings*/>** – параметры подключения к каталогу пользователей
  - ***rootPath*** – LDAP путь к домену, в котором находятся пользователи системы
  - ***userName*** – имя сервисной учетной записи для изменения параметров профиля пользователей (“serviceKeyBox”)
  - ***password*** – пароль сервисной учетной записи
- **<*adAccessControlSettings*/>** – параметры проверки подлинности Windows для доступа к web-сервисам Рутокен KeyBox.
  - ***adminGroup*** – указатель группы администраторов системы. Необходимо указать группу, члены которой получат полный доступ на управление системой. Значение по умолчанию – KeyBox Admins.
  - ***helpDeskOperatorGroup*** – указатель группы операторов системы. Необходимо указать группу, члены которой получат доступ на управление смарт-картами пользователей. Значение по умолчанию – KeyBox Help Desk Operators.
  - ***userGroup*** – указатель группы пользователей системы. Необходимо указать группу, члены которой получат доступ к сервису самообслуживания Рутокен KeyBox. Значение по умолчанию – KeyBox Users.
- **<*authorization*/>** – параметры авторизации для web-сервисов Рутокен KeyBox
  - ***allow roles*** – путь к группам безопасности, члены которых обладают правом доступа к Консоли управления Рутокен KeyBox. Задайте down-level logon name (имя регистрации в ранних версиях Windows вида DOMAIN\GroupName) для группы Администраторов и Операторов Рутокен KeyBox, определенных в теге **<*adAccessControlSettings*/>**. Например, для группы KeyBox Admins домена keybox.local следует указать путь KEYBOX\KeyBox Admins.

Важная информация

Помимо аутентификации в сервисах Рутокен KeyBox средствами Windows (доступ предоставляется только членам указанных групп безопасности) существует возможность аутентификации пользователей с помощью персональных сертификатов. Подробнее о настройках аутентификации по сертификатам см. в разделе **Настройка аутентификации в web-сервисах Рутокен KeyBox**.

Сохраните изменения в файле **keybox\Web.config**.

Ниже приведен пример отредактированного содержимого файла для Web.config с пояснениями для каждого раздела (тэга), параметры которого были изменены.

...

- *<managementConsoleSettings cpClientCertificateEKUs="" cp2ClientCertificateEKUs="" showMsPkiSettings="true" showCpPkiSettings="false" showCp2PkiSettings="false" showEASettings="false" showEnforceSmartCardLogonSetting="true" />*
- *<adPersistenceSettings path="LDAP://CN=Rutoken,CN=KeyBox,DC=keybox,DC=local" userName="serviceKeyBox" password="Password1" cryptoAlgName="Rijndael" cryptoKey="1506331e899e3431a8434e1bbd906233b26e2d4ce2e4dd792cc9168c0225c1e3"/>*
- *<adUserCatalogSettings rootPath="LDAP://DC=keybox,DC=local" userName="serviceAD" password="Password1"/>*
- *<adAccessControlSettings adminGroup="KeyBox Admins" helpDeskOperatorGroup="KeyBox Help Desk Operators" userGroup="KeyBox Users" />*

…

- *<authorization>*
- *<deny users="?" />*
- *<allow roles="KEYBOX\KeyBox Help Desk Operators, KEYBOX\KeyBox Admins"/>*
- *<deny users="*" />*
- *</authorization>*

…

Пояснения к разделу ***managementConsoleSettings***:

Т.к. КриптоПРО УЦ не используются в данной конфигурации, то значения параметров *cpClientCertificateEKUs* и *cp2ClientCertificateEKUs* не заданы. Для параметра *showMsPkiSettings* определено значение "true", т.к. в качестве удостоверяющего центра будет использоваться только Microsoft CA. По этой же причине значения параметров *showCpPkiSettings* и *showCp2PkiSettings* – "false". Интеграция с Indeed Enterprise Authentication также не рассматривается, поэтому значение параметра *showEASettings=" false"*. Параметр *showEnforceSmartCardLogonSetting* имеет значение *"true"*, т.к. в случае использования Active Directory как каталога пользователей, опция, позволяющая включить принудительное использование смарт-карты для входа в ОС, может быть использована при выпуске смарт-карты некоторым группам пользователей.

Пояснения к разделу ***adPersistenceSettings***:

В домене keybox.local создано хранилище данных системы – контейнер Rutoken с подконтейнером KeyBox. Поэтому полный путь к хранилищу данных системы в параметре *path* имеет вид *"LDAP://CN=Rutoken, CN=KeyBox,DC=keybox,DC=local"*. Сервисная учетная запись, обладающая правами на работу с хранилищем данных – serviceKeyBox, поэтому значение параметра *userName="serviceKeyBox"*, пароль этой сервисной записи – *"Password1"*. Выбранный алгоритм шифрования данных в хранилище – *Rijndael*, поэтому значение параметра *cryptoAlgName="Rijndael"*, а сам ключ шифрования указан в параметре *cryptoKey*.

Пояснения к разделу ***adUserCatalogSettings***:

Пользователями системы Рутокен KeyBox являются все пользователи домена keybox.local, поэтому путь к каталогу пользователей в параметре *rootPath* имеет вид "LDAP://DC=keybox,DC=local". Сервисная учетная запись, обладающая правами на изменение параметров в профиле пользователей Active Directory – *serviceAD*, её пароль – *Password1*, соответственно, значение параметра *userName="serviceAD"*, а *password="Password1"*.

Пояснения к разделу ***adAccessControlSettings***:

Значения всех параметров оставлены без изменений, т.к. использование альтернативных групп безопасности для доступа к web-сервисам не предполагается.

Пояснения к разделу ***authorization***:

Доступ к приложению Management Console имеют пользователи, входящие в группы KeyBox Help Desk Operators, KeyBox Admins. Down-level logon name этих групп указаны в качестве значений параметра allow roles="KEYBOX\KeyBox Help Desk Operators, KEYBOX\KeyBox Admins".

Параметры для конфигурации, когда хранилище данных Рутокен KeyBox расположено в Microsoft SQL, а каталог пользователей системы расположен в Центре Регистрации КриптоПРО УЦ 1.5

После заполнения обязательного тэга <managementConsoleSettings/> удалите из файла конфигурации следующие строки:

<adPersistenceSettings path="LDAP://LDAP_PATH" userName="ACCOUNT_NAME" password="ACCOUNT_PASSWORD" cryptoAlgName="Rijndael" cryptoKey="CRYPTO_KEY"/>

<adUserCatalogSettings rootPath="LDAP://LDAP_ROOT_PATH" userName="ACCOUNT_NAME" password="ACCOUNT_PASSWORD"/>

<!--<cp2UserCatalogSettings raServiceUrl="RA_SERVICE_URL" clientCertificateThumbprint="CLIENT_CERTIFICATE_THUMBPRINT"/>-->

<adAccessControlSettings adminGroup="KeyBox Admins" helpDeskOperatorGroup="KeyBox Help Desk Operators" userGroup="KeyBox Users" />

Заполните нижеследующие тэги:

- ***<sqlPersistenceSettings/>*** – параметры подключения к хранилищу данных Рутокен KeyBox в среде Microsoft SQL. Раскомментируйте SQL реализацию хранилища данных Рутокен KeyBox удалив тег **<! -- …. -->** и укажите значения следующих параметров:
  - ***connectionString*** – строка подключения к базе данных. Может содержать параметры:
    - ***Server*** (имя рабочей станции с установленным сервером SQL)

- ***Intitial Catlog*** (имя базы данных, созданной на этапе создания хранилища)
- ***Intergrated Security*** (способ подключения к базе: **true** – используется учетная запись Windows, **false** - используется учетная запись на SQL. В случае использования SQL учетной записи необходимо указать ее логин и пароль в полях **User ID** и **Password**.)

- ***cryptoAlgName*** – название алгоритма шифрования, который Вы выбрали на этапе генерации ключа шифрования при помощи утилиты KeyBox.KeyGen.exe.
- ***cryptoKey*** – ключ шифрования, полученный при помощи утилиты KeyBox.KeyGen.exe.

Пример заполненного раздела:

- *<sqlPersistenceSettings connectionString="Server=KeyBoxSrv;Initial Catalog=KeyBox;Integrated Security=false;User ID=KeyBoxSQL;Password=Password1" cryptoAlgName="Rijndael" cryptoKey="e01e29030a79e68a8080f0b65603b9bc9b8b94ddc93f3496026fd0b90d080f66"/>*

Важная информация

Параметры строки подключения в разделе sqlPersistenceSettings connectionString могут отличаться в зависимости от используемой редакции Microsoft SQL Server (Standard или Express) и варианта установки (на одной рабочей станции с сервером Рутокен KeyBox или на отдельной рабочей станции).

В случае использования SQL Express параметр подключения к серверу необходимо задавать в формате <имя сервера SQL >\<имя инстанса SQL>: *sqlPersistenceSettings connectionString="Server=KeyBoxSrv\SQLEXPRESS;Initial Catalog=KeyBox;Integrated Security=false;User ID=KeyBoxSQL;Password=Password1"*

В случае использования SQL Standard имя инстанса SQL указывать не нужно: *<sqlPersistenceSettings connectionString="Server=KeyBoxSrv;Initial Catalog=KeyBox;Integrated Security=false;User ID=KeyBoxSQL;Password=Password1"*

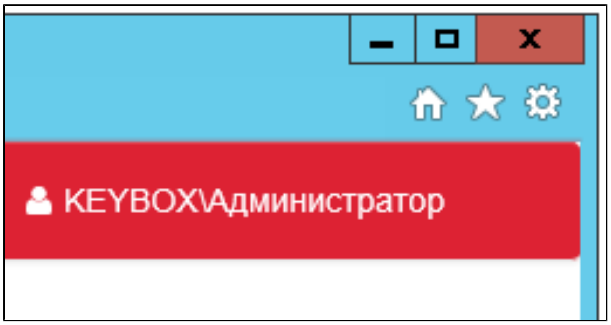
- ***<cpUserCatalogSettings/>*** – параметры подключения к каталогу пользователей, расположенному в Центре Регистрации КриптоПРО УЦ 1.5
  - ***raServiceUrl*** – строка для подключения к Центру Регистрации КриптоПРО УЦ 1.5
  - ***clientCertificateThumbprint*** – отпечаток сертификата, который будет использоваться для подключения к Центру Регистрации КриптоПРО для просмотра списка пользователей (сертификат роли Выпуск сертификатов KeyBox).
  - ***logonNameAttribute*** – атрибут имени пользователя, по которому определяется его уникальность при аутентификации в web-сервисах KeyBox (например, «EMail» или «Common name»). Если не указан, то будет использоваться значение 1.2.840.113549.1.9.1 (EMail). Если в свойствах пользователя не будет указан адрес электронной почты, Рутокен KeyBox не сможет найти такого пользователя.

Пример заполненного раздела:

- *<cpUserCatalogSettings raServiceUrl="https://RA/RA.asp" clientCertificateThumbprint="105b459fe5cbce021e00a92223880256894b841a" logonNameAttribute="2.5.4.3"> </cpUserCatalogSettings>*

Также в данном разделе определяется структура каталогов Центра Регистрации КриптоПРО УЦ 1.5. В соответствии с указанной в файле конфигурации структурой будет осуществляться назначение политик выпуска смарт-карт Рутокен KeyBox. См. **Создание структуры каталогов для распространения политик выпуска смарт-карт.**

- ***<certificateAccessControlSettings/>*** – параметры доступа к web-сервисам Рутокен KeyBox по персональным сертификатам пользователей.
  - ***adminFilter*** – фильтр администраторов системы. В качестве значения задается OID или отпечаток (Thumbprint) сертификата роли Администратор KeyBox.
  - ***helpDeskOperatorFilter*** – фильтр администраторов системы. В качестве значения задается OID сертификата роли Оператор KeyBox.
  - ***userFilter*** – фильтр пользователей системы. В качестве значения задается OID сертификата роли Пользователь KeyBox.
  - ***logonNameAttribute*** – атрибут имени пользователя. Определяет формат отображения имени пользователя в верхнем правом углу приложения web-сервиса:



Если не указан, то будет использоваться значение 1.2.840.113549.1.9.1 (EMail). Если в свойствах пользователя не будет указан адрес электронной почты, Рутокен KeyBox не сможет найти такого пользователя.

Возможные значения:

- Идентификатор (OID) "2.5.4.3" (Общее имя) – для отображения общего имени пользователя (если включено в сертификат, предоставленный пользователем для аутентификации web-сервисе).
- "upn" – для отображения UPN-имени пользователя (если включено в сертификат, предоставленный пользователем для аутентификации в web-сервисе).

Пример заполненного раздела:

- *<certificateAccessControlSettings adminFilter="EKUs:1.3.6.1.4.1.2.2.34.3" helpDeskOperatorFilter="EKUs: 1.3.6.1.4.1.2.2.34.4" userFilter="EKUs:1.3.6.1.4.1.2.2.34.5" logonNameAttribute="2.5.4.3"/>*

В примере указаны по одному идентификатору для каждого фильтра. Для указания нескольких значений одного типа (например, два идентификатора роли для фильтра администратора) синтаксис будет выглядеть так:

adminFilter="EKUs:OID1,OID2"

Это означает, что система предоставит доступ пользователю (в данном примере Администратору KeyBox) только в том случае, если в сертификате, предоставленным этим пользователем будут перечислены оба идентификатора.

Если необходимо фильтровать пользователей по какому-либо одному из нескольких OID, то синтаксис будет следующим:

adminFilter="EKUs:OID1;EKUs:OID2"

Помимо фильтрации по идентификатору роли поддерживается и фильтрация по отпечатку (Thumbprint):

adminFilter="Thumbprint:05eac3725eaa791f18ef45118ff3fa269c4d706f"

Важная информация

При указании отпечатка в фильтре доступ к web-приложению будет предоставлен только одному человеку – обладателю сертификата с указанным отпечатком. Второго такого сертификата быть не может.

Для предоставления доступа по отпечатку сертификата двум и более пользователям необходимо указать отпечатки сертификатов этих пользователей через точку с запятой:

adminFilter="Thumbprint:123;Thumbprint:345"

Если пользователь попадает под действие нескольких фильтров (например, в его сертификате есть идентификаторы роли "Оператор KeyBox" и "Администратор KeyBox"), то система аутентифицирует его с наивысшими правами (т.е. как Администратора).

- ***<filters/>*** – типы фильтров доступа по персональным сертификатам web-приложения. Раскомментируйте фильтр авторизации удалив тег **<!-- … -->**:
- *<filters>*
- *<add type="IndeedCM.Web.ManagementConsole.CertificateAuthorizationFilter, IndeedCM.Web.ManagementConsole"/>*
- *</filters>*

- ***<authentication mode/>*** – режим проверки подлинности для доступа к web-приложению.
  - Раскомментируйте секцию *<authentication mode="None" />* удалив тег *<!-- … -->*
  - Закомментируйте секцию *<authentication mode="Windows"/>* используя тег *<!-- … -->*.

Пример заполненного раздела:

- *<authentication mode="None"/>*
- *<!--<authentication mode="Windows" />-->*

- ***<authorization/>*** – параметры авторизации пользователей. Применимы в случае использования проверки подлинности Windows и расположением пользователей в Active Directory. Закомментируйте раздел используя тег **<!-- … -->**.

Пример закомментированного раздела:

- <!-- <authorization>
  - <deny users="?" />
  - <allow roles="DOMAIN_NAME\KeyBox Help Desk Operators, DOMAIN_NAME\KeyBox Admins"/>
  - <deny users="*" />
- </authorization>-->

Сохраните изменения в файле конфигурации.

Откройте файл keybox\unity.config и внесите следующие изменения:

- Закомментируйте реализацию хранилища данных в Active Directory, используя тег **<!-- …. -->**:

<!--

<register type="ICardRepository" mapTo="IndeedCM.Persistence.AD.CardRepository, IndeedCM.Persistence.AD" />

<register type="IUserDataRepository" mapTo="IndeedCM.Persistence.AD.UserDataRepository, IndeedCM.Persistence.AD" />

<register type="IPolicyRepository" mapTo="IndeedCM.Persistence.AD.PolicyRepository, IndeedCM.Persistence.AD" />

<register type="ICardTypeRepository" mapTo="IndeedCM.Persistence.AD.CardTypeRepository, IndeedCM.Persistence.AD" />

<register type="ILicenseRepository" mapTo="IndeedCM.Persistence.AD.LicenseRepository, IndeedCM.Persistence.AD" />

-->

- Раскомментируйте SQL реализацию хранилища данных, удалив тег **<!-- …. -->**:

<register type="ICardRepository" mapTo="IndeedCM.Persistence.SQL.CardRepository, IndeedCM.Persistence.SQL" />

<register type="IUserDataRepository" mapTo="IndeedCM.Persistence.SQL.UserDataRepository, IndeedCM.Persistence.SQL" />

<register type="IPolicyRepository" mapTo="IndeedCM.Persistence.SQL.PolicyRepository, IndeedCM.Persistence.SQL" />

<register type="ICardTypeRepository" mapTo="IndeedCM.Persistence.SQL.CardTypeRepository, IndeedCM.Persistence.SQL" />

<register type="ILicenseRepository" mapTo="IndeedCM.Persistence.SQL.LicenseRepository, IndeedCM.Persistence.SQL" />

- Закомментируйте реализацию каталога пользователей в Active Directory, используя тег **<!-- .... -->**:
  - *<!--<register type="IUserCatalog" mapTo="IndeedCM.UserCatalog.AD.UserCatalog, IndeedCM.UserCatalog.AD" />-->*
- Раскомментируйте реализацию каталога пользователей КпритоПРО УЦ 1.5, удалив тег **<!-- .... -->**:
  - *<register type="IUserCatalog" mapTo="IndeedCM.UserCatalog.CP.UserCatalog, IndeedCM.UserCatalog.CP" />*
- Закомментируйте доменную реализацию контроля доступа, используя тег **<!-- .... -->**:
  - *<!--<register type="ILoggedOnUserInfo" mapTo="IndeedCM.AccessControl.AD.LoggedOnUserInfoProvider, IndeedCM.AccessControl.AD" />-->*
- Раскомментируйте реализацию контроля доступа по сертификатам, удалив тег **<!-- .... -->**:
  - <register type="ILoggedOnUserInfo" mapTo="IndeedCM.AccessControl.Certificate.LoggedOnUserInfoProvider, IndeedCM.AccessControl.Certificate" />
- Сохраните изменения и закройте файл.

Первый этап конфигурирования приложения Management Console завершен. Чтобы убедиться в правильности настройки приложения выполните вход на страницу приложения под ролью Администратор KeyBox с аутентификацией по сертификату. Для этого необходимо любым удобным способом выпустить соответствующий сертификат и поместить его на смарт-карту. Подключите смарт-карту к рабочей станции и убедитесь в том, что в хранилище личных сертификатов пользователя отображается сертификат роли Администратор KeyBox. Откройте Internet Explorer и укажите адрес приложения Management Console: **https://<имя сервера Рутокен KeyBox>/keybox.**
Если проверка подлинности и параметры SSL в Диспетчере служб IIS для приложения keybox указаны верно, то в браузере появится окно выбора сертификата пользователя (из числа тех, что расположены в личном хранилище пользователя):

Выберите нужный сертификат, нажмите **ОК** и укажите PIN-код смарт-карты. В случае возникновения ошибки HTTP Error 403 следует проверить значения в разделе **Улучшенный ключ**, перечисленные в используемом для входа сертификате и сравнить с теми, что указаны в файле конфигурации в качестве значения параметра **adminFilter**. Также следует проверить настройки **Диспетчера служб IIS** для

приложения keybox (SSL включен и требуется предоставление клиентского сертификата, разрешено только анонимное подключение).
Если вход выполнен успешно, осуществите поиск пользователя в разделе **Служба поддержки** – **Поиск пользователя**, тем самым проверив подключение к каталогу пользователей КриптоПРО УЦ 1.5. Ожидаемый результат – найти любого пользователя, существующего в **Центре Регистрации КриптоПРО УЦ.** В качестве контейнера, в котором расположен пользователь, должно быть указано имя удостоверяющего центра:

Для проверки соединения с базой данных SQL перейдите в раздел **Конфигурация** и добавьте файл лицензии или типа карты. Ожидаемый результат – лицензия или тип карты добавились и отображаются в соответствующем меню раздела Конфигурация.

Теперь можно перейти ко второму этапу – созданию структуры каталогов, на которые будут распространяться политики выпуска смарт-карт.

Создание структуры каталогов для распространения политик выпуска смарт-карт

В варианте установки Рутокен KeyBox с используемым в качестве хранилища данных Рутокен KeyBox каталогом Active Directory назначение политик происходит на объекты службы каталогов (контейнеры и подразделения), в которых находятся пользователи. Если Active Directory нет, и пользователи находятся в хранилище Центра Регистрации КриптоПРО 1.5, структуры каталогов в котором нет, то политика выпуска смарт-карт может быть только одна. Область действия такой политики – корневой контейнер с именем УЦ, т.е. действие политики распространяется на всех пользователей этого УЦ.

Для создания структуры каталогов Рутокен KeyBox использует сведения из профиля пользователя УЦ КриптоПРО 1.5. Это название организации, подразделения, должность и т.п. Поддерживаются все поля, имеющиеся в КриптоПРО УЦ 1.5. Наиболее удобным вариантом распределения пользователей является их группировка по названию компании, подразделению или географическим признакам (страна, город, регион). Ниже пример информации о пользователе КриптоПРО УЦ 1.5:

Используя эти данные можно создать следующую структуру для распространения политики:

- **CryptoPRO-1.5**
  - **Компания АКТИВ**
    - **Рутокен**
      - **KeyBox**
        - **Ведущие сотрудники**

Где CryptoPRO-1.5 – имя центра сертификации КриптоПРО, с каталогом пользователей которого работает Рутокен KeyBox.

На основе этой структуры существует возможность создавать разные политики для пользователей, в свойствах которых задано:

- только имя организации (Компания АКТИВ)
- имя организации и подразделение (Компания АКТИВ\Рутокен)

- имя организации, подразделение и отдел (Компания АКТИВ\Рутокен\KeyBox)
- имя организации, подразделение, отдел и группа в отделе (Компания АКТИВ\Рутокен\KeyBox\Ведущие сотрудники)

Логика применения политик такова: если есть политика, действующая на организацию и есть политика, действующая на подразделение в этой организации, то для пользователя, расположенного в подразделении будет действовать политика этого подразделения, а не организации.

Необходимая структура каталогов задается на этапе конфигурации системы в файлах web.config всех приложений и также в файле конфигурации IndeedCM.CardMonitor.exe.config. Структура каталогов определяется в разделе **cpUserCatalogSettings**.

В разделе ***<layout>*** перечисляются идентификаторы (**OID**) полей, заполняемых при создании пользователя КриптоПРО УЦ 1.5, с которыми необходимо работать системе Рутокен KeyBox. Для получения необходимых значений **OID** следует обратиться в Центр регистрации КриптоПРО УЦ (**Свойства ЦР – Политики – Политики имен**).

Например:

```
<layout>

<level componentOid="2.5.4.10" componentPos="1"/>

<level componentOid="2.5.4.11" componentPos="1"/>

<level componentOid="2.5.4.11" componentPos="2"/>

<level componentOid="2.5.4.11" componentPos="3"/>

</layout>
```

В приведенном примере действие политик будет распространяться только на пользователей, у которых заполнены поля “Организация” (OID 2.5.4.10) и “Подразделение” (OID 2.5.4.11). При этом полей “Подразделение” в свойствах одного пользователя может быть несколько, и они будут вложены как в поле “Организация”, так и друг в друга в рамках одной Организации. Степень вложенности задается параметром **componentPos**.

<level componentOid="2.5.4.10" componentPos="1"/> – поле “Организация” на первом уровне. Это значит, что после корневого контейнера с именем УЦ Рутокен KeyBox будет распространять действие политики на пользователей, в свойствах которых заполнено поле “Организация”.

<level componentOid="2.5.4.11" componentPos="1"/> – поле “Подразделение” на первом уровне, но т.к. в строке выше на первом уровне указано поле “Организация”, то это подразделение будет вложено в организацию.

<level componentOid="2.5.4.11" componentPos="2"/> – Ещё одно подразделение, которое должно быть расположено внутри подразделения с componentPos="1" (поэтому его позиция 2).

<level componentOid="2.5.4.11" componentPos="3"/> – третье подразделение, которое будет вложено в предыдущее подразделение (поэтому его позиция 3).

Описанная выше конструкция позволяет задать такие конфигурации:

- Корневой контейнер/Организация1/Подразделение1/Подразделение 1.1/Подразделение/1.1.1
  - Пример: **ИмяУЦ/Компания АКТИВ/Рутокен/KeyBox/Ведущие сотрудники**
- Корневой контейнер/Организация2/Подразделение2/Подразделение 2.1/Подразделение/2.1.1
  - Пример: **ИмяУЦ/ООО "Компания"/Бухгалтерия/Специалисты/Специалисты категории 1**

Важная информация

Обе конструкции могут быть одновременно использованы в одном файле конфигурации. В этом случае предполагается что один центр регистрации КриптоПРО обслуживает пользователей двух организаций, у каждой из которых есть свои подразделения. И, соответственно, у части пользователей такого ЦР в полях “Организация” и “Подразделение” будут указаны названия организации-1 и подразделений-1, а участи пользователей будут указаны названия организации-2 и подразделений-2.

В соответствии со структурой, заданной в разделе ***<layout>*** необходимо задать имена объектов и их расположение используя теги ***<containers>*** и ***<container>***.

<containers>

<container id="1" name="Компания АКТИВ"> 1

<containers>

<container id="1" name="Рутокен"> 2

<containers>

<container id="1" name="KeyBox"> 3

<containers>

<container id="2" name="Ведущие сотрудники"> 4

</containers>

</container>

</containers>

```
</container>

</containers>

</container>

</containers>
```

Теперь все необходимые настройки для приложения keybox (Management Console) заданы. Ниже приведены все описанные разделы файла конфигурации в заполненном виде для рассматриваемой конфигурации:

```
<managementConsoleSettings cpClientCertificateEKUs="1.3.6.1.4.1.2.2.34.1" cp2ClientCertificateEKUs="
1.3.6.1.5.5.7.3.2" showMsPkiSettings="false" showCpPkiSettings="true" showCp2PkiSettings="false"
showEASettings="false" showEnforceSmartCardLogonSetting="false" />

<sqlPersistenceSettings connectionString="Server=KeyBoxSrv;Initial Catalog=KeyBox;Integrated Security=false;
User ID=KeyBoxSQL;Password=Password1" cryptoAlgName="Rijndael" cryptoKey="
e01e29030a79e68a8080f0b65603b9bc9b8b94ddc93f3496026fd0b90d080f66"/>

<cpUserCatalogSettings raServiceUrl="https://w2k3r/RA/RA.asp" clientCertificateThumbprint="
105b459fe5cbce021e00a92223880256894b841a" logonNameAttribute="2.5.4.3">

<layout>

<level componentOid="2.5.4.10" componentPos="1"/>

<level componentOid="2.5.4.11" componentPos="1"/>

<level componentOid="2.5.4.11" componentPos="2"/>

<level componentOid="2.5.4.11" componentPos="3"/>

</layout>

<containers>

<container id="1" name="Компания АКТИВ"> 1

<containers>

<container id="1" name="Рутокен"> 2
```

```
<containers>

<container id="1" name="KeyBox"> 3

<containers>

<container id="2" name="Ведущие сотрудники"> 4

</containers>

</container>

</containers>

</container>

</containers>

</container>

</containers>

</cpUserCatalogSettings>

<certificateAccessControlSettings adminFilter="EKUs:1.3.6.1.4.1.2.2.34.3" helpDeskOperatorFilter="EKUs:
1.3.6.1.4.1.2.2.34.4" userFilter="EKUs:1.3.6.1.4.1.2.2.34.5" logonNameAttribute="2.5.4.3"/>

<filters>

<add type="IndeedCM.Web.ManagementConsole.CertificateAuthorizationFilter, IndeedCM.Web.
ManagementConsole"/>

</filters>

<authentication mode="None"/>

<!--<authentication mode="Windows" />-->

<!--<authorization>

<deny users="?" />

<allow roles="DOMAIN_NAME\KeyBox Help Desk Operators, DOMAIN_NAME\KeyBox Admins"/>
```

<deny users="" />*

</authorization>-->

Параметры для конфигурации, когда хранилище данных Рутокен KeyBox расположено в Microsoft SQL, а каталог пользователей системы расположен в Центре Регистрации КриптоПРО УЦ 2.0

После заполнения обязательного тэга <managementConsoleSettings/> удалите из файла конфигурации следующие строки:

<adPersistenceSettings path="LDAP://LDAP_PATH" userName="ACCOUNT_NAME" password="ACCOUNT_PASSWORD" cryptoAlgName="Rijndael" cryptoKey="CRYPTO_KEY"/>

<adUserCatalogSettings rootPath="LDAP://LDAP_ROOT_PATH" userName="ACCOUNT_NAME" password="ACCOUNT_PASSWORD"/>

<!--<cp2UserCatalogSettings raServiceUrl="RA_SERVICE_URL" clientCertificateThumbprint="CLIENT_CERTIFICATE_THUMBPRINT"/>-->

<adAccessControlSettings adminGroup="KeyBox Admins" helpDeskOperatorGroup="KeyBox Help Desk Operators" userGroup="KeyBox Users" />

Заполните нижеследующие тэги:

- ***<sqlPersistenceSettings/>*** – параметры подключения к хранилищу данных Рутокен KeyBox в среде Microsoft SQL. Раскомментируйте SQL реализацию хранилища данных Рутокен KeyBox удалив тег **<! -- …. -->** и укажите значения следующих параметров:
  - ***connectionString*** - строка подключения к базе данных. Может содержать параметры:
    - ***Server*** (имя рабочей станции с установленным сервером SQL)
    - ***Intitial Catlog*** (имя базы данных, созданной на этапе создания хранилища)
    - ***Intergrated Security*** (способ подключения к базе: **true** – используется учетная запись Windows, **false** - используется учетная запись на SQL. В случае использования SQL учетной записи необходимо указать ее логин и пароль в полях **User ID** и **Password**.)
  - ***cryptoAlgName*** - название алгоритма шифрования, который Вы выбрали на этапе генерации ключа шифрования при помощи утилиты KeyBox.KeyGen.exe.
  - ***cryptoKey*** - ключ шифрования, полученный при помощи утилиты KeyBox.KeyGen.exe.

Пример заполненного раздела:

- *<sqlPersistenceSettings connectionString="Server=KeyBoxSrv;Initial Catalog=KeyBox;Integrated Security=false;User ID=KeyBoxSQL;Password=Password1" cryptoAlgName="Rijndael" cryptoKey="e01e29030a79e68a8080f0b65603b9bc9b8b94ddc93f3496026fd0b90d080f66"/>*

Важная информация

Параметры строки подключения в разделе sqlPersistenceSettings connectionString могут отличаться в зависимости от используемой редакции Microsoft SQL Server (Standard или Express) и варианта установки (на одной рабочей станции с сервером Рутокен KeyBox или на отдельной рабочей станции).

В случае использования SQL Express параметр подключения к серверу необходимо задавать в формате <имя сервера SQL >\<имя инстанса SQL>: *sqlPersistenceSettings connectionString="Server=KeyBoxSrv\SQLEXPRESS;Initial Catalog=KeyBox;Integrated Security=false;User ID=KeyBoxSQL;Password=Password1"*

В случае использования SQL Standard имя инстанса SQL указывать не нужно: *<sqlPersistenceSettings connectionString="Server=KeyBoxSrv;Initial Catalog=KeyBox;Integrated Security=false;User ID=KeyBoxSQL;Password=Password1"*

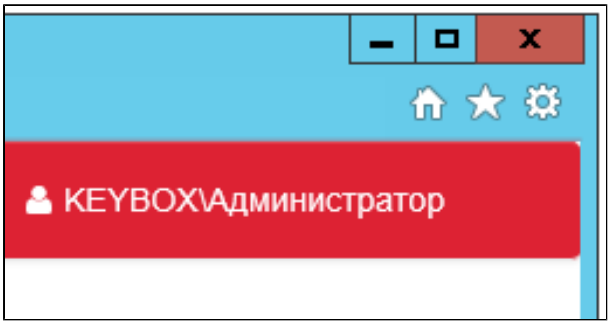
- ***<cp2UserCatalogSettings/>*** – параметры подключения к каталогу пользователей, расположенному в Центре Регистрации КриптоПРО УЦ 2.0
  - ***raServiceUrl*** - строка для подключения к Центру Регистрации КриптоПРО УЦ 2.0
  - ***clientCertificateThumbprint*** - отпечаток сертификата, который будет использоваться для подключения к Центру Регистрации КриптоПРО для просмотра списка пользователей (сертификат роли Выпуск сертификатов KeyBox).
  - ***logonNameAttribute*** - атрибут имени пользователя, по которому определяется его уникальность при аутентификации в web-сервисах KeyBox (например, «EMail» или «Common name»). Если не указан, то будет использоваться значение 1.2.840.113549.1.9.1 (EMail). Если в свойствах пользователя не будет указан адрес электронной почты, Рутокен KeyBox не сможет найти такого пользователя.

Пример заполненного раздела:

<cpUserCatalogSettings raServiceUrl="https:///RA/RA.asp" clientCertificateThumbprint="105b459fe5cbce021e00a92223880256894b841a" logonNameAttribute="2.5.4.3"> </cpUserCatalogSettings>

- ***<certificateAccessControlSettings/>*** - параметры доступа к web-сервисам Рутокен KeyBox по персональным сертификатам пользователей.
  - ***adminFilter*** – фильтр администраторов системы. В качестве значения задается OID или отпечаток (Thumbprint) сертификата роли Администратор KeyBox.
  - ***helpDeskOperatorFilter*** – фильтр администраторов системы. В качестве значения задается OID сертификата роли Оператор KeyBox.
  - ***userFilter*** – фильтр пользователей системы. В качестве значения задается OID сертификата роли Пользователь KeyBox.

- ***logonNameAttribute*** – атрибут имени пользователя. Определяет формат отображения имени пользователя в верхнем правом углу приложения web-сервиса:



Если не указан, то никакое имя пользователя отображаться не будет.

Возможные значения:

- Идентификатор (OID) "2.5.4.3" (Общее имя) - для отображения общего имени пользователя (если включено в сертификат, предоставленный пользователем для аутентификации web-сервисе).
- "upn" - для отображения UPN-имени пользователя (если включено в сертификат, предоставленный пользователем для аутентификации в web-сервисе).

Пример заполненного раздела:

- *<certificateAccessControlSettings adminFilter="Thumbprint: 6AE353D02332D5B41E6CC9DE57FB27CD0AA55EDC" helpDeskOperatorFilter="Thumbprint: 6AE353D02332D5B41E6CC9DE57FB27CD0AA55EDC" userFilter="EKUs:1.2.643.2.2.34.6" logonNameAttribute="2.5.4.3"/>*

В примере указаны по одному идентификатору для каждого фильтра. Для указания нескольких значений одного типа (например, два идентификатора роли для фильтра администратора) синтаксис будет выглядеть так:

adminFilter="EKUs:OID1,OID2"

Это означает, что система предоставит доступ пользователю (в данном примере Администратору KeyBox) только в том случае, если в сертификате, предоставленным этим пользователем будут перечислены оба идентификатора.

Если необходимо фильтровать пользователей по какому-либо одному из нескольких OID, то синтаксис будет следующим:

adminFilter="EKUs:OID1;EKUs:OID2"

Помимо фильтрации по идентификатору роли поддерживается и фильтрация по отпечатку (Thumbprint):

adminFilter="Thumbprint:05eac3725eaa791f18ef45118ff3fa269c4d706f"

Важная информация

При указании отпечатка в фильтре доступ к web-приложению будет предоставлен только одному человеку – обладателю сертификата с указанным отпечатком. Второго такого сертификата быть не может.

Для предоставления доступа по отпечатку сертификата двум и более пользователям необходимо указать отпечатки сертификатов этих пользователей через точку с запятой:

adminFilter="Thumbprint:123;Thumbprint:345"

Если пользователь попадает под действие нескольких фильтров (например, в его сертификате есть идентификаторы роли "Оператор KeyBox" и "Администратор KeyBox"), то система аутентифицирует его с наивысшими правами (т.е. как Администратора).

- **<*filters*/>** – типы фильтров доступа по персональным сертификатам web-приложения. Раскомментируйте фильтр авторизации удалив тег **<!-- … -->**:

<filters>

<add type="IndeedCM.Web.ManagementConsole.CertificateAuthorizationFilter, IndeedCM.Web.ManagementConsole"/>

</filters>

- **<*authentication mode*/>** – режим проверки подлинности для доступа к web-приложению.
  - Раскомментируйте секцию <*authentication mode="None"* /> удалив тег <!-- … -->
  - Закомментируйте секцию <*authentication mode="Windows"*/> используя тег <!-- … -->.

Пример заполненного раздела:

<authentication mode="None"/>

<!--<authentication mode="Windows" />->

- **<*authorization*/>** – параметры авторизации пользователей. Применимы в случае использования проверки подлинности Windows и расположением пользователей в Active Directory. Закомментируйте раздел используя тег **<!-- … -->**.

Пример закомментированного раздела:

<!-- <authorization>

<deny users="?" />

<allow roles="DOMAIN_NAME\KeyBox Help Desk Operators, DOMAIN_NAME\KeyBox Admins"/>

<deny users="*" />

</authorization>-->

Сохраните изменения в файле конфигурации.

Откройте файл keybox\unity.config и внесите следующие изменения:

- Закомментируйте реализацию хранилища данных в Active Directory, используя тег **<!-- …. -->**:

<!--

<register type="ICardRepository" mapTo="IndeedCM.Persistence.AD.CardRepository, IndeedCM.Persistence.AD" />

<register type="IUserDataRepository" mapTo="IndeedCM.Persistence.AD.UserDataRepository, IndeedCM.Persistence.AD" />

<register type="IPolicyRepository" mapTo="IndeedCM.Persistence.AD.PolicyRepository, IndeedCM.Persistence.AD" />

<register type="ICardTypeRepository" mapTo="IndeedCM.Persistence.AD.CardTypeRepository, IndeedCM.Persistence.AD" />

<register type="ILicenseRepository" mapTo="IndeedCM.Persistence.AD.LicenseRepository, IndeedCM.Persistence.AD" />

-->

- Раскомментируйте SQL реализацию хранилища данных, удалив тег **<!-- …. -->**:

<register type="ICardRepository" mapTo="IndeedCM.Persistence.SQL.CardRepository, IndeedCM.Persistence.SQL" />

<register type="IUserDataRepository" mapTo="IndeedCM.Persistence.SQL.UserDataRepository, IndeedCM.Persistence.SQL" />

<register type="IPolicyRepository" mapTo="IndeedCM.Persistence.SQL.PolicyRepository, IndeedCM.Persistence.SQL" />

<register type="ICardTypeRepository" mapTo="IndeedCM.Persistence.SQL.CardTypeRepository, IndeedCM.Persistence.SQL" />

<register type="ILicenseRepository" mapTo="IndeedCM.Persistence.SQL.LicenseRepository, IndeedCM.Persistence.SQL" />

- Закомментируйте реализацию каталога пользователей в Active Directory, используя тег ***<!-- .... -->***:
  - *<!--<register type="IUserCatalog" mapTo="IndeedCM.UserCatalog.AD.UserCatalog, IndeedCM.UserCatalog.AD" />-->*
- Раскомментируйте реализацию каталога пользователей КпритоПРО УЦ 1.5, удалив тег ***<!-- .... -->***:
  - *<register type="IUserCatalog" mapTo="IndeedCM.UserCatalog.CP.UserCatalog, IndeedCM.UserCatalog.CP" />*
- Закомментируйте доменную реализацию контроля доступа, используя тег ***<!-- .... -->***:
  - *<!--<register type="ILoggedOnUserInfo" mapTo="IndeedCM.AccessControl.AD.LoggedOnUserInfoProvider, IndeedCM.AccessControl.AD" />-->*
- Раскомментируйте реализацию контроля доступа по сертификатам, удалив тег ***<!-- .... -->***:
  - <register type="ILoggedOnUserInfo" mapTo="IndeedCM.AccessControl.Certificate.LoggedOnUserInfoProvider, IndeedCM.AccessControl.Certificate" />
- Сохраните изменения и закройте файл.

Конфигурирование Self-Service

Сервис **keyboxservice** предназначен для самостоятельного управления пользователем его смарт-картами при подключении из внутренней сети компании. Файлы конфигурации по умолчанию располагаются в %SystemDrive%:\inetpub\wwwroot\keyboxservice.

Откройте от имени администратора на редактирование файл **keyboxservice\Web.config**. Структура файла схожа с таковой в файле **keybox\Web.config.** В зависимости от конфигурации Рутокен KeyBox, укажите параметры подключения к хранилищу данных системы (***adPersistenceSettings*** или ***sqlPersistenceSettings***), каталогу пользователей (***adUserCatalogSettings***, ***cpUserCatalogSettings*** или ***cp2UserCatalogSettings***). Значения всех параметров данных разделов должны совпадать с теми, что указаны в файле конфигурации приложения **Management Console**.

Настройте параметры доступа к приложению (***adAccessControlSettings*** или ***certificateAccessControlSettings*** (включая раздел ***<filters>***)) и метод аутентификации (***authentication mode*** и ***authorization***):

- В случае использования Windows-аутентификации укажите группу пользователей, члены которой будут иметь доступ к приложению. По умолчанию это KeyBox Users.
- В случае использования аутентификации по персональным сертификатам укажите перечень назначений (**EKU**, Extended Key Usage) или отпечатков (**Thumbpint**) сертификатов, обладателям которых будет предоставлен доступ.

Сохраните изменения в файле.

Файл **unity.config** приложения **keyboxservice** идентичен файлу **unity.config** приложения **keybox** выбранной конфигурации. Скопируйте его с заменой из %Systemdrive%\inetpub\wwwroot\keybox\ в %Systemdrive%\inetpub\wwwroot\keyboxservice\.

Конфигурирование Remote Self-service

Сервис **keyboxremote** предназначен для самостоятельного управления пользователем его смарт-картами при подключении из сети Интернет. Файлы конфигурации по умолчанию располагаются в %SystemDrive%:\inetpub\wwwroot\keyboxremote.

Откройте от имени администратора на редактирование файл **keyboxremote\Web.config**. Структура файла схожа с таковой в файле **keybox\Web.config**. В зависимости от конфигурации Рутокен KeyBox, укажите параметры подключения к хранилищу данных системы (***adPersistenceSettings*** или ***sqlPersistenceSettings***), каталогу пользователей (***adUserCatalogSettings***, ***cpUserCatalogSettings*** или ***cp2UserCatalogSettings***). Значения всех параметров данных разделов должны совпадать с теми, что указаны в файле конфигурации приложения Management Console. Сохраните изменения в файле.

Файл unity.config приложения KeyBox Remote Self Service необходимо изменить, в соответствии с используемой конфигурацией Рутокен KeyBox. По аналогии с файлом конфигурации сервиса Management Console **keybox\unity.config** определите в теге ***<container>*** разделы для работы с хранилищем данных Рутокен KeyBox и каталогом пользователей. Сохраните изменения в файле.

Конфигурирование CredprovAPI

Сервис CredprovApi предназначен для разблокировки смарт-карт пользователей. Файлы конфигурации по умолчанию располагаются в %SystemDrive%:\inetpub\wwwroot\credprovapi.

Откройте от имени администратора на редактирование файл **credprovapi\Web.config**. Структура файла схожа с таковой в файле **keybox\Web.config**. В зависимости от конфигурации Рутокен KeyBox, укажите параметры подключения к хранилищу данных системы (***adPersistenceSettings*** или ***sqlPersistenceSettings***), каталогу пользователей (***adUserCatalogSettings***, ***cpUserCatalogSettings*** или ***cp2UserCatalogSettings***). Значения всех параметров данных разделов должны совпадать с теми, что указаны в файле конфигурации приложения Management Console. Сохраните изменения в файле.

Файл **unity.config** приложения credprovapi необходимо изменить, в соответствии с используемой конфигурацией Рутокен KeyBox. По аналогии с файлом конфигурации сервиса Management Console **keybox\unity.config** определите в теге ***<container>*** разделы для работы с хранилищем данных Рутокен KeyBox и каталогом пользователей. Сохраните изменения в файле.

Конфигурирование сервиса Card Monitor

Сервис Card Monitor предназначен для выполнения операций по контролю за обращением смарт-карт в системе Рутокен KeyBox. Сервис предоставляет следующие возможности:

- отзыв карт удаленных пользователей;

- отзыв временных карт с истекшим сроком действия;
- рассылка почтовых уведомлений администраторам и пользователям системы:
  - Истечение срока действия сертификатов пользователей, хранящихся на карте;
  - Одобрение/отклонение выпуска карты;
  - Одобрение/отклонение обновления сертификатов на карте;
  - Одобрение/отклонение замены карты.

Утилиту KeyBox Card Monitor следует запускать на сервере Рутокен KeyBox используя Планировщик заданий Windows. Настройте ежедневный запуск утилиты KeyBox.CardMonitor.exe (желательно на период, когда активность пользователей минимальна, например, в ночные часы).

Важная информация

Учетная запись, от имени которой создается задача в Планировщике Windows, должна обладать правами Локального администратора (Local Admins) и правами администратора Рутокен KeyBox (KeyBox Admins).

В свойствах задачи укажите **Выполнять вне зависимости от регистрации пользователя и Выполнить с наивысшими правами**.

Откройте от имени администратора на редактирование файл %ProgramFiles%\Rutoken KeyBox\CardMonitor\IndeedCM.CardMonitor.exe.config. Структура файла схожа с таковой в файле keybox\Web.config. В зависимости от конфигурации Рутокен KeyBox, укажите параметры подключения к хранилищу данных системы (***adPersistenceSettings*** или ***sqlPersistenceSettings***) и каталогу пользователей (***adUserCatalogSettings***, ***cpUserCatalogSettings*** или ***cp2UserCatalogSettings***). Значения всех параметров данных разделов должны совпадать с теми, что указаны в файле конфигурации приложения Management Console.

Если в качестве каталога пользователей системы используется Active Directory, то необходимо в разделе ***<adAccessControlSettings/>*** указать только группу безопасности KeyBox Admins. Сохраните изменения в файле.

Файл **unity.config** приложения Card Monitor необходимо изменить, в соответствии с используемой конфигурацией Рутокен KeyBox. По аналогии с файлом конфигурации сервиса Management Console keybox\unity.config определите в теге ***<container>*** разделы для работы с хранилищем данных Рутокен KeyBox, каталогом пользователей и параметрами доступа. Сохраните изменения в файле.

Шифрование данных в файлах конфигурации web-приложений

Информация, содержащаяся в файлах конфигурации всех сервисов Рутокен KeyBox может быть зашифрована при помощи утилиты **KeyBox.ConfigEncryptor.exe**, входящей в состав дистрибутива Рутокен KeyBox (располагается в KeyBox.Server\Misc\EncryptConfigs). Утилита позволяет шифровать /расшифровывать следующие секции конфигурационных файлов:

- adPersistenceSettings

- sqlPersistenceSettings
- adUserCatalogSettings
- cpUserCatalogSettings
- cp2UserCatalogSettings
- managementConsoleSettings
- adAccessControlSettings
- certificateAccessControlSettings
- filters

Шифрование осуществляется при помощи машинного ключа шифрования Microsoft .NET (NetFrameworkConfigurationKey). Алгоритм шифрования – RSA.

Важная информация

Расшифровка данных возможна только на той рабочей станции, на которой данные были зашифрованы.

Для шифрования фрагмента файла конфигурации запустите утилиту KeyBox.ConfigEncryptor.exe в командной строке от имени Администратора (Run as Administrator) с параметром **/encrypt**, указанием пути к файлу конфигурации и названием секции, данные которой необходимо зашифровать.

Пример:

KeyBox.ConfigEncryptor.exe /encrypt "C:\inetpub\wwwroot\keybox\web.config" "sqlPersistenceSettings"

В случае успешного шифрования появится сообщение:

Configuration section has been encrypted successfully.

После выполнения шифрования указанный раздел в файле конфигурации примет следующий вид:

- *<sqlPersistenceSettings configProtectionProvider="RsaProtectedConfigurationProvider">*
  - *<EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element" xmlns="http://www.w3.org/2001/04/xmlenc#">*
    - *<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />*
    - *<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">*
      - *<EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">*
        - *<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />*
        - *<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">*
          - *<KeyName>Rsa Key</KeyName>*
        - *</KeyInfo>*

- <CipherData>
  - <CipherValue>bQnCb0FPULbSLzzDI
    /Q+kIIh53p+EDdsMIMZNRIL7B05CLEQeBkvqIe9niBd8RFs7QO3J4pM71j8hioHCU6qmjYepPvKjlZW
    /OAN3jEE7XrBaQlKKJuh8dk9HkVO
    /tH3Vl4qHoJP2gRsUNQYF4vZrNotZwev2rIncgnAqtnPy/DyIyNR
    /o74tYHWb4IMcBFB6fHcVnZXsbvbSL+uU95Ugos/tWmSTNbmTpNCECo
    /J1l00k8IUm/Qg==</CipherValue>
  - </CipherData>
- </EncryptedKey>
- </KeyInfo>
- <CipherData>
  - <CipherValue>HyI3jD2IGDD1hx5CHt/ZCQi17vLztpe9+rx/VucR+Mlaq
    /dW+ECkaRGoFeMtUNmxzDS2f/AdQ88ubsfyOB987DWkXcAixgG8II
    /BvDP92KhMyEyPKr8CePOxmBUOJe1L0fGfvXAWfaz8
    /oCjguG25eMH2pnr4ldRoglhFNlm6cRgQ1aNjKt+BAY6ixdlPmkguwzfA
    /icC27O5351h62cTIeYEWmOjO92yD1jybnYQbyjS+r3x9E5BgM+YvA6vVO9VV4jdQC
    /yJYR1HSQfnVByJKuhtjGbrXD6xj60eHvsJWZo89tH8sGMf+bcHjEEs13WVNo0KdxUx9Ok50EHlRvHhd12TrfT
    /CipherValue>
- </CipherData>
- </EncryptedData>
- </sqlPersistenceSettings>

Шифрование остальных секций происходит аналогичным образом.

Важная информация

Рекомендуется выполнять шифрование всех используемых секций (из числа поддерживаемых утилитой) всех файлов конфигурации. Закомментированные тегом <!-- …--> секции не шифруются.

Для расшифровки фрагмента файла конфигурации запустите утилитуKeyBox.ConfigEncryptor.exe в командной строке от имени Администратора (Run as Administrator) с параметром **/decrypt**, указанием пути к файлу конфигурации и названием секции, данные которой необходимо расшифровать.

Пример:

KeyBox.ConfigEncryptor.exe /decrypt "C:\inetpub\wwwroot\keybox\web.config" "sqlPersistenceSettings"

В случае успешного шифрования появится сообщение:

Configuration section has been decrypted successfully.

После расшифровки указанный раздел в файле конфигурации примет исходный (до момента шифрования) вид.

Для массового шифрования и расшифровки секций всех файлов конфигурации удобно использовать пакетные файлы encryptConfigs.bat и decryptConfigs.bat (расположены в каталоге с утилитой шифрования дистрибутива Рутокен KeyBox) соответственно. По умолчанию файлы настроены на шифрование и расшифровку разделов ***adUserCatalogSettings*** и ***adPersistenceSettings*** в файлах конфигурации всех web-сервисов Рутокен KeyBox. Ниже приведено содержание файла **encryptConfigs.bat**:

- *rem management console*
- *IndeedCm.Config.Encryptor /encrypt "C:\inetpub\wwwroot\icm\web.config" "adUserCatalogSettings"*
- *IndeedCm.Config.Encryptor /encrypt "C:\inetpub\wwwroot\icm\web.config" "adPersistenceSettings"*

- *rem self-service*
- *IndeedCm.Config.Encryptor /encrypt "C:\inetpub\wwwroot\icmservice\web.config" "adUserCatalogSettings"*
- *IndeedCm.Config.Encryptor /encrypt "C:\inetpub\wwwroot\icmservice\web.config" "adPersistenceSettings"*

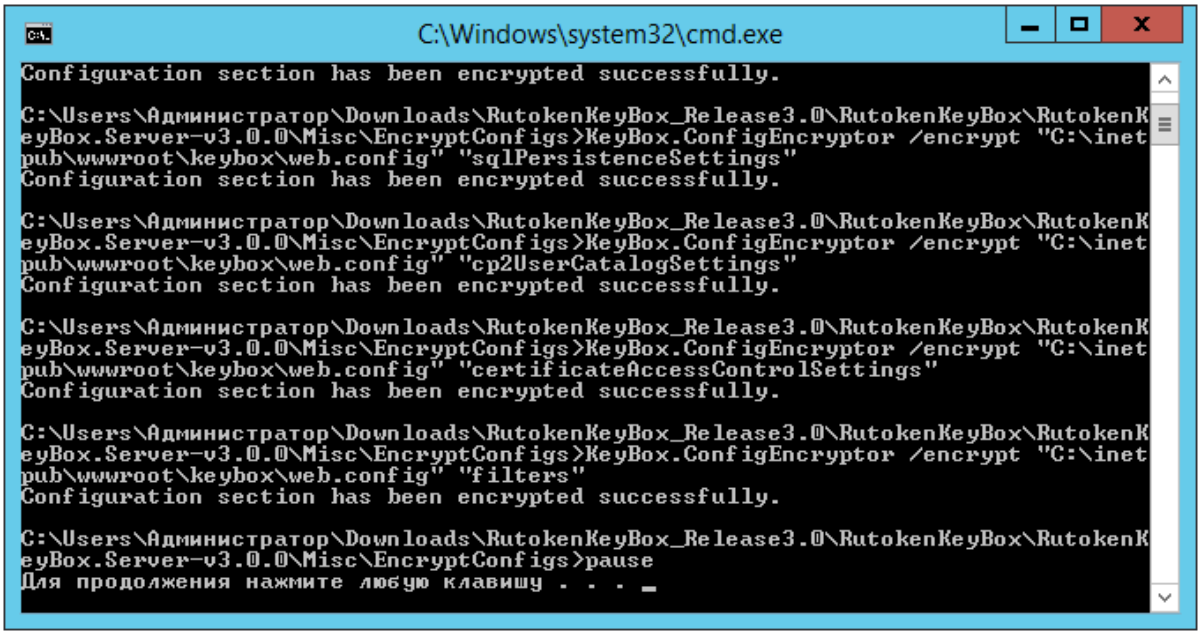
- *rem remote self-service*
- *IndeedCm.Config.Encryptor /encrypt "C:\inetpub\wwwroot\icmremote\web.config" "adUserCatalogSettings"*
- *IndeedCm.Config.Encryptor /encrypt "C:\inetpub\wwwroot\icmremote\web.config" "adPersistenceSettings"*

- *rem credential provider API*
- *IndeedCm.Config.Encryptor /encrypt "C:\inetpub\wwwroot\credprovapi\web.config" "adUserCatalogSettings"*
- *IndeedCm.Config.Encryptor /encrypt "C:\inetpub\wwwroot\credprovapi\web.config" "adPersistenceSettings"*

- *rem card monitor*
- *IndeedCm.Config.Encryptor /encrypt "C:\Program Files\IndeedCM\CardMonitor\IndeedCM.CardMonitor.exe.config" "adUserCatalogSettings"*
- *IndeedCm.Config.Encryptor /encrypt "C:\Program Files\IndeedCM\CardMonitor\IndeedCM.CardMonitor.exe.config" "adPersistenceSettings"*

- *pause*

Вы можете добавить в содержание файла параметры (путь к файлу конфигурации и название секции) для шифрования необходимых секций всех файлов конфигурации сразу. Сохраните изменения и запустите пакетный файл. Ниже приведен результат выполнения пакетного файла, в результате которого были зашифрованы разделы ***managementConsoleSettings***, ***sqlPersistenceSettings***, ***cp2UserCatalogSettings***, ***certificateAccessControlSettings*** и ***filters*** файла конфигурации приложения Management Console (keybox\Web.config):



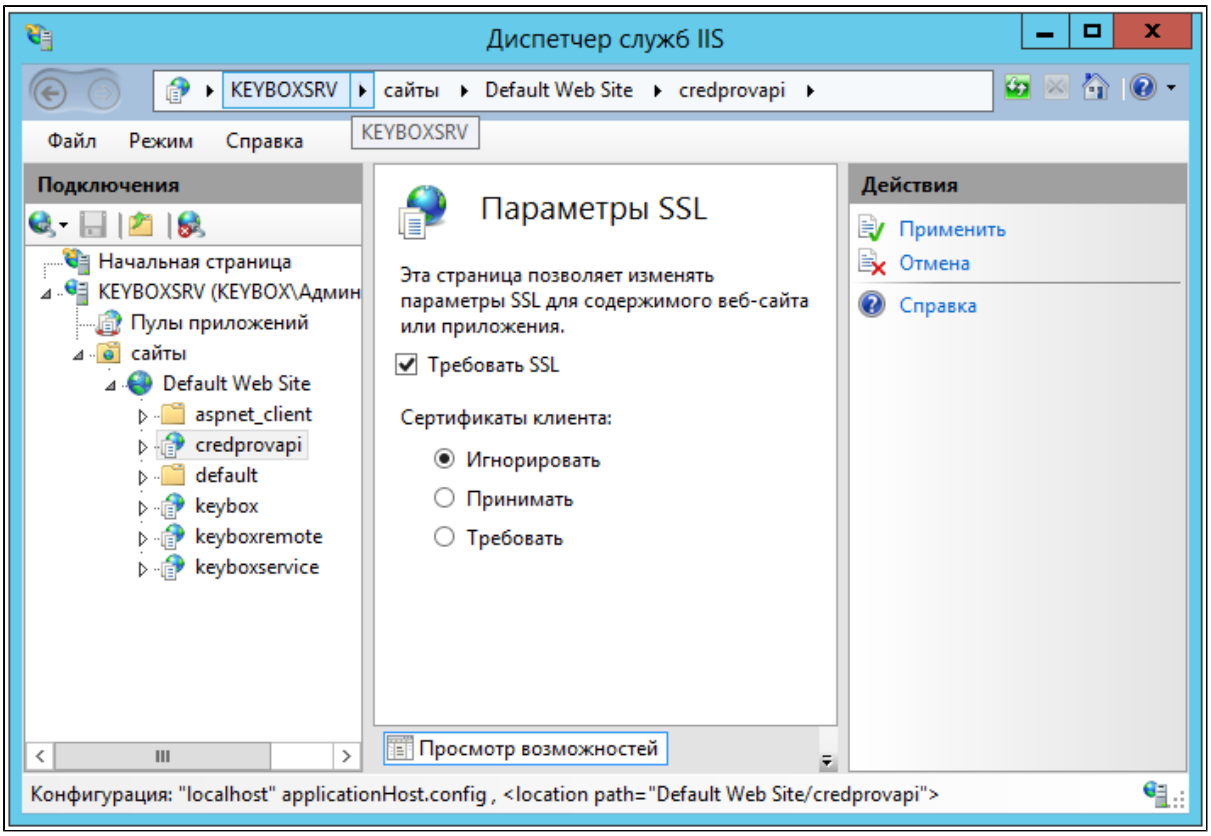
Настройка online-разблокировки смарт-карт

Разблокировка смарт-карты в режиме Online подразумевает, что рабочая станция пользователя, к которой подключена заблокированная смарт-карта имеет соединение с сервером Рутокен KeyBox. Соединение с сервером необходимо для проведения аутентификации пользователя при помощи ответов на секретные вопросы.

Для связи рабочих станций пользователей с сервером Рутокен KeyBox при online-разблокировке смарт-карт рекомендуется использовать защищенное соединение.

Выполните настройки соединения для сервиса **credprovapi**: в качестве сертификата **SSL** в настройках **IIS** необходимо указать сертификат рабочей станции, на которой развернут сервер Рутокен KeyBox.

В **Параметрах SSL** (SSL Settings) приложения **credprovapi** для сертификатов клиента должен быть указан параметр **Игнорировать** (Ignore):



В зависимости от конфигурации, в которой развернута система Рутокен KeyBox способы включения Online разблокировки смарт-карта на рабочих станциях пользователей различаются.

Включение Online разблокировки смарт-карт в домене Windows

Для включения возможности online-разблокировки смарт-карт пользователей необходимо настроить соответствующую групповую политику. Данная политика должна распространяться на рабочие станции пользователей системы Рутокен KeyBox.

Выполните следующие действия, чтобы добавить административный файл шаблона:

- Откройте консоль **Управление групповой политикой** (Group Policy Management).
- В дереве окна консоли создайте новый объект групповой политики, или выберите существующий. Вызовите контекстное меню и выберите пункт **Изменить** (Edit).
- В открывшемся **Редакторе объектов групповой политики** (Group Policy Management Editor) выберите **Конфигурация компьютера** (Computer Configuration) > **Политики** (Policies) > **Административные шаблоны** (Administrative Templates). Вызовите контекстное меню, и выберите пункт **Добавление и удаление шаблонов** (Add/Remove Templates).
- В диалоге **Добавление и удаление шаблонов** (Add/Remove Templates) нажмите **Добавить** (Add).
- Укажите путь к шаблону KeyBox.Client.adm (располагается в \KeyBox.Client.Tools\Misc\ дистрибутива). Выбранный шаблон отображается в списке **Текущие шаблоны политики** (Current Policy Templates). Закройте диалог **Добавление и удаление шаблонов** (Add/Remove Templates).
- В редакторе объектов групповой политики в ветке **Административные шаблоны** (Administrative Templates) > **Классические административные шаблоны** (Classic Administrative Templates) отображается новый объект KeyBox, содержащий добавленный шаблон.
- Включите политику **Сервер разблокировки смарт-карт** и укажите её значения:

- в параметре URL сервиса укажите ссылку на компонент credprovapi, размещенный на сервере Рутокен KeyBox., например, https://keyboxsrv.test.local/credprovapi;
- в параметре Проверять сертификат сервера установите значение Да (значение по умолчанию), если необходимо проводить проверку подлинности сертификата сервера. Установите Нет, если проверку подлинности проводить не требуется.

- Свяжите данный объект группой политики с группой, членами которой являются рабочие станции пользователей системы Рутокен KeyBox.
- Нажмите **Применить** (Apply) и выполните обновление политик.

Включение Online разблокировки смарт-карт вне домена Windows

В случае, когда сервер Рутокен KeyBox и рабочие станции пользователей находятся вне домена Windows, путь к приложению credprovapi необходимо прописать в реестре каждой клиентской рабочей станции. Для этого создайте файл реестра (.reg) со следующим содержанием:

- *[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\IndeedCM\Client]*
- *"CredProvAPIURL"="*
- *"DisableServerCertificateChecking"=dword:00000000*

В параметре **CredProvAPIURL** следует указать адрес приложения credprovapi на сервере Рутокен KeyBox. В параметре **DisableServerCertivicateChecking** установите значение 0 (значение по умолчанию), если необходимо проводить проверку подлинности сертификата сервера Рутокен KeyBox. Установите 1 (dword: 00000001), если проверку подлинности проводить не требуется.

Ниже приведен пример файла для сервера Рутокен KeyBox с именем машины keyboxsrv и включенной проверкой подлинности сертификата сервера:

- *[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\IndeedCM\Client]*
- *"CredProvAPIURL"="https://keyboxsrv/credprovapi"*
- *"DisableServerCertificateChecking"=dword:00000000*

Настройка аутентификации в web-сервисах

В зависимости от окружения, в котором развернут Рутокен KeyBox существует несколько способов аутентификации пользователей в web-сервисах системы:

Каталог пользователей	Способ аутентификации
Active Directory	Windows -аутентификация; Аутентификация по персональным сертификатам пользователей любого доступного УЦ
КриптоПро УЦ	Аутентификация по персональным сертификатам пользователей.

Каталог пользователей	Способ аутентификации
	Сертификаты должны быть выданы УЦ, выступающим в роли каталога пользователей

Аутентификация Windows

Осуществляться по принадлежности пользователей к группам безопасности Windows (по умолчанию это группы KeyBox Admins, KeyBox Help Desk Operators, KeyBox Users). Такой способ аутентификации применим в случае, когда хранилище пользователей системы KeyBox расположено в Active Directory.

Аутентификация по персональным сертификатам пользователей

Для каждого web-сервиса Рутокен KeyBox в файлах конфигурации определяется перечень значений поля Улучшенный ключ (EKU, Extended Key Usage) или отпечатков (Thumbpint) сертификатов, обладателям которых будет предоставлен доступ. Сертификаты могут быть выпущены как удостоверяющим центром Microsoft, так и КриптоПро.

Создание сертификата аутентификации сервера КриптоПро УЦ 1.5

Этим сертификатом будут шифроваться данные, передаваемые с клиента на сервер Рутокен KeyBox и обратно.

Для создания сертификата необходимо на сервере Рутокен KeyBox сформировать запрос, который затем будет обработан УЦ КриптоПро.

- Запустите оснастку **Сертификаты** (Certificates) для локального компьютера на сервере Рутокен KeyBox.
- Перейдите в раздел **Личные** (Personal), щелкните правой кнопкой мыши и выберите **Все задачи** (All Tasks) -> **Дополнительные операции** (Advanced Operations) -> **Создать настраиваемый запрос** (Create Custom Request).
- В окне **Выбор политики регистрации сертификатов** (Select Certificate Enrollment Policy) выберите **Настраиваемый запрос**. **Продолжить без политики регистрации** (Custom request. Proceed without enrollment policy).
- В поле **Шаблон** (Template) укажите **Старый ключ (без шаблона)** (No template) Legacy key.
- Укажите **Формат запроса** (Request format) **PKCS #10**.
- В окне **Сведения о сертификате** (Certificate Information) разверните пункт **Подробности** (Details) создаваемого запроса и затем перейдите его в **Свойства** (Propetries).
- Перейдите на вкладку **Субъект** (Subject), выберите **Общее имя** (Common name), укажите в поле **Значение** (Value) полное имя рабочей станции, на которой установлен сервер Рутокен KeyBox и затем нажмите кнопку **Добавить** (Add).
- Перейдите на вкладку **Расширения** (Extensions), разверните пункт **Использование ключа** (Key Usage) и добавьте следующие назначения сертификата:

- **Шифрование данных** (Data encipherment)
- **Цифровая подпись** (Digital signature)
- **Шифрование ключей** (Key encipherment)
- **Неотрекаемость** (No repudiation)

- Разверните раздел **Расширенное использование ключа (политики применения)** (Extended Key Usage (application policies)). Выберите **Проверка подлинности сервера** (Server authentication) и нажмите кнопку **Добавить** (Add)
- Перейдите на вкладку **Закрытый ключ** (Private Key) и разверните пункт **Поставщик службы шифрования** (Cryptographic Service Provider). Выберите **КриптоПро CSP**, убрав при этом все прочие **CSP**.
- Разверните пункт **Тип ключа** (Key type) и укажите допустимое действие для закрытого ключа сертификата **Обмен** (Exchange).
- Нажмите кнопку **Применить** (Apply) и затем **Далее** (Next) для создания запроса. Сохраните запрос в файл и перенесите его на машину с установленным приложением **Обработка запроса сертификата Web-сервера ЦР**.
- Запустите приложение **Обработка запроса сертификата Web-сервера ЦР**, укажите путь к файлу запроса, перенесенному с сервера Рутокен KeyBox и параметры сохранения сертификата.
- Нажмите **Далее** и завершите выпуск сертификата.
- Перенесите выпущенный сертификат на сервер Рутокен KeyBox и установите его в личное хранилище компьютера используя **КриптоПро CSP (Сервис->Установить личный сертификат**).
- Укажите путь к файлу сертификата. Убедитесь в том, что выбран сертификат той рабочей станции, на которой установлен сервер Рутокен KeyBox.
- Укажите, что введенное имя задает ключевой контейнер компьютера и отметьте опцию **Найти контейнер автоматически**. После этого в качестве хранилища контейнера определится **Реестр**, нажмите **Далее** и завершите установку сертификата.
- Запустите оснастку **Сертификаты** (Certificates) для локального компьютера на сервере Рутокен KeyBox, перейдите в раздел **Личные** (Personal) -> **Сертификаты** (Certificates) кликните правой кнопкой мыши на сертификате, установленному при помощи **КриптоПро CSP**, выберите **Все задачи** (All tasks) – **Управление закрытыми ключами...** (Manage Private Keys...), нажмите **Добавить** (Add), укажите локальную группу **IIS_IUSRS** и выставите права Полный доступ (Full Control) и **Чтение** (Read). Нажмите **Применить** (Apply).

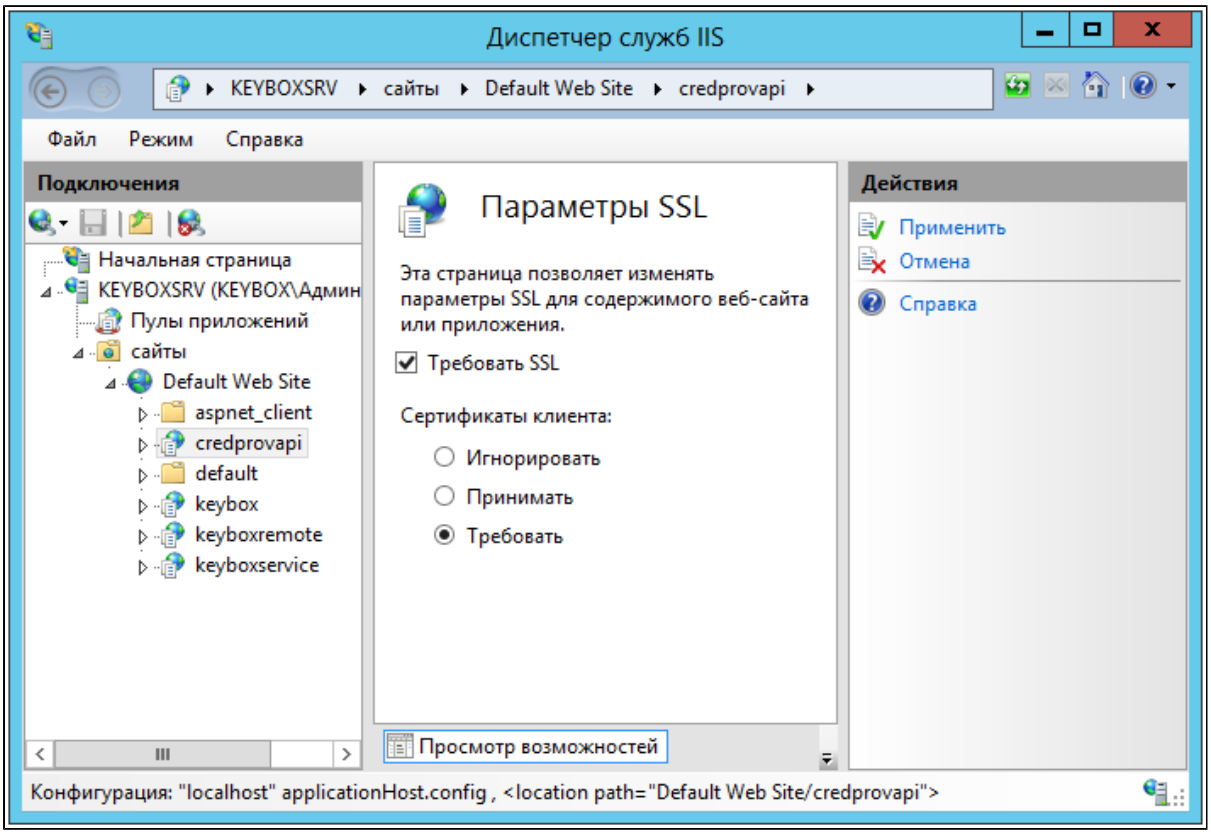
Создание сертификата аутентификации сервера КриптоПро УЦ 2.0

- Зарегистрируйте нового пользователя КриптоПро УЦ, указав в качестве имени пользователя полное имя рабочей станции, на которой установлен сервер Рутокен KeyBox.
- С рабочей станции, на которой установлен сервер Рутокен KeyBox, выполните вход в личный кабинет пользователя КриптоПро УЦ по идентификатору и временному паролю учетной записи сервера.
- Создайте запрос на сертификат, указав шаблон **KeyBox Service User**, криптопровайдер **Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider**, использование ключа – **Подпись**.
- Отправьте созданный запрос в Центр Регистрации.
- Дождитесь одобрения запроса Оператором Центра Регистрации.
- Перейдите в раздел **Запросы - Изготовление** личного кабинета пользователя КриптоПро.

- Загрузите и сохраните изготовленный сертификат.
- Установите полученный сертификат в личное хранилище компьютера используя **КриптоПро CSP (Сервис->Установить личный сертификат)**.
- Укажите путь к файлу сертификата. Убедитесь в том, что выбран сертификат той рабочей станции, на которой установлен сервер Рутокен KeyBox.
- Укажите, что введенное имя задает ключевой контейнер компьютера и отметьте опцию **Найти контейнер автоматически**. После этого в качестве хранилища контейнера определится **Реестр**, нажмите **Далее** и завершите установку сертификата.
- Запустите оснастку **Сертификаты** (Certificates) для локального компьютера на сервере Рутокен KeyBox, перейдите в раздел **Личные** (Personal) -> **Сертификаты** (Certificates) кликните правой кнопкой мыши на сертификате, установленному при помощи **КриптоПро CSP**, выберите **Все задачи** (All tasks) - **Управление закрытыми ключами...** (Manage Private Keys...), нажмите **Добавить** (Add), укажите локальную группу **IIS_IUSRS** и выставите права **Полный доступ** (Full Control) и **Чтение** (Read). Нажмите **Применить** (Apply).

Настройка Диспетчера служб IIS для аутентификации по сертификатам пользователей

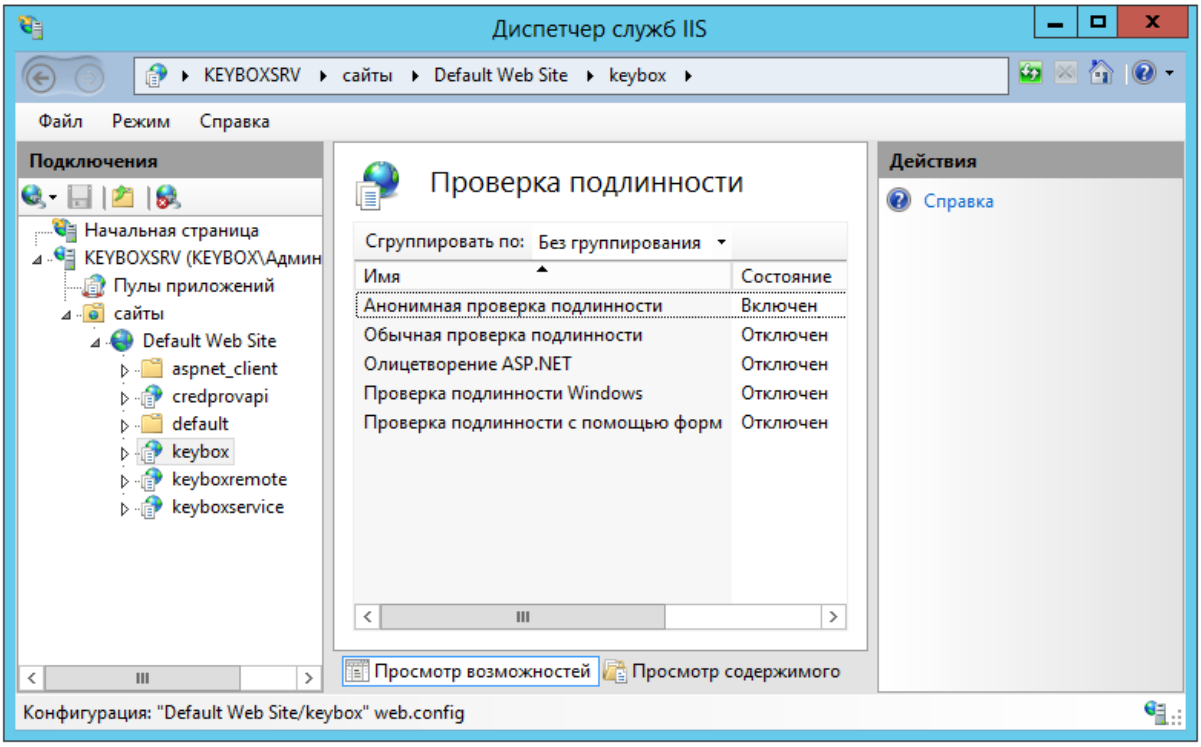
- Добавьте сертификат серверной аутентификации в **IIS** в разделе **Привязки** (Bindings).
- Настройте параметры проверки подлинности для приложений Рутокен KeyBox:
  - Включите использование **SSL** для приложений credprovapi (Сервис разблокировки смарт-карт), keybox (Management Console) и keyboxservice (Self Service) в Диспетчере IIS: **Параметры SSL** -> **Требовать SSL** (SSL Settings -> Require SSL), установите опцию **Требовать** (Require) и примените внесенные изменения:



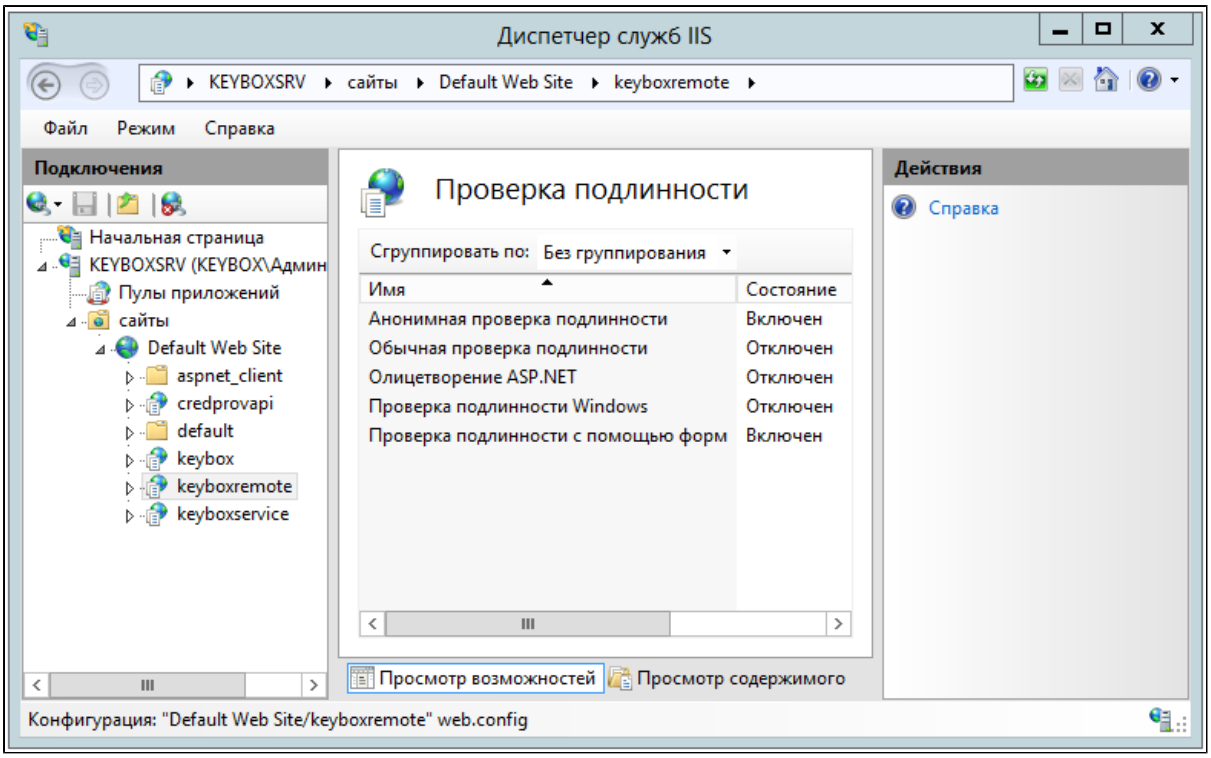
- Для приложения **keyboxremote** (Remote Self Service) включите использование SSL-соединения и установите опцию **Принимать** (Apply).

- Определите настройки проверки подлинности для приложений **keybox** и **keyboxservice** (Management Console и Self Service соответственно):

  - В разделе **Проверка подлинности** (Authentication) **Диспетчера служб IIS** отключите **Проверку подлинности Windows** (Windows Authentication) и включите **Анонимную проверку подлинности** (Anonymous Authentication):



- Для приложения **keyboxremote** (Remote Self Service) необходимо включить **Анонимную проверку подлинности** (Anonymous Authentication) и **Проверку подлинности с помощью форм** (Forms Authentication). Все остальные способы проверки подлинности необходимо отключить:



Установка клиентской части

Компоненты Рутокен KeyBox Middleware устанавливаются на рабочих местах операторов службы поддержки и на рабочих станциях пользователей. В зависимости от типа устройств, используемых в организации, на рабочую станцию оператора и пользователя устанавливаются те или иные компоненты Middleware. Например, для работы с устройствами Рутокен необходимо установить компонент KeyBox. Rutoken.Middleware, а для устройств ESMART – KeyBox.ESMART.Middleware.

Компонент Client Tools устанавливается только на рабочие станции пользователей.

Важная информация

На всех рабочих станциях пользователей должны быть установлены драйвера и сервисные утилиты, тех смарт-карт и считывателей, которые будут использоваться с системой Рутокен KeyBox. Данное ПО не входит в комплект поставки Рутокен KeyBox.

Установка Рутокен KeyBox Middleware

Запустите файл KeyBox.Middleware.msi из дистрибутива Рутокен KeyBox и выполните установку, следуя указаниям мастера.

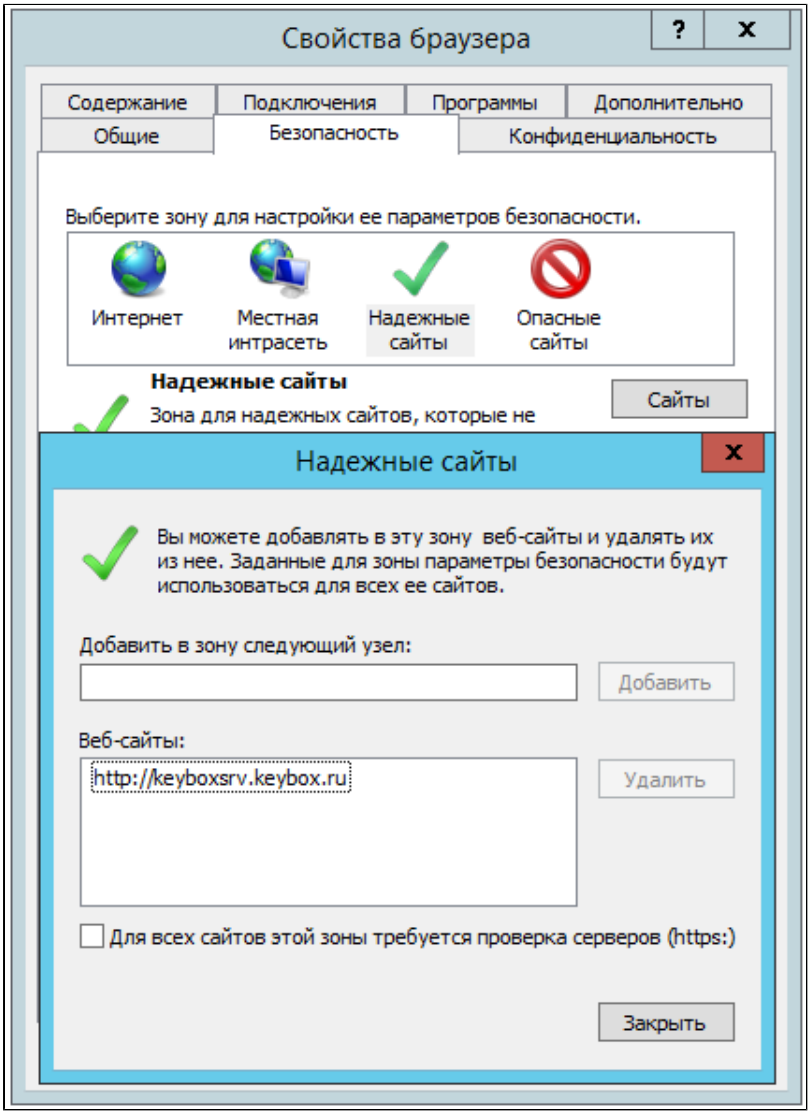
Установка Рутокен KeyBox Client Tools

Запустите файл KeyBox.ClientTools.msi из дистрибутива Рутокен KeyBox и выполните установку, следуя указаниям мастера.

Настройка Internet Explorer для работы с web-приложениями Рутокен KeyBox

Прежде, чем приступить к работе с web-сервисами Рутокен KeyBox, необходимо настроить параметры безопасности в браузере Internet Explorer.

Добавьте адрес сервера Рутокен KeyBox в зону надежных сайтов. Для этого перейдите в настройки безопасности Internet Explorer (**Свойства браузера - Безопасность**), выберите зону **Надежные сайты** и нажмите кнопку **Сайты**. Укажите узел, на котором установлен Рутокен KeyBox Server и нажмите **Добавить**. Ниже приведен пример настроек, где keyboxsrv.keybox.ru - полное имя сервера на котором установлен Рутокен KeyBox, для подключения к которому требуется использовать протокол **https**.



Сбор программных логов

Наличие программных логов позволяет специалистам службы поддержки оперативно локализовать причины возможных проблемных ситуаций и принять меры к их устранению. Сбор программных логов осуществляется с помощью утилиты Indeed GetLog, поставляемой в составе дистрибутива (располагается в каталоге Get Log).

Для сбора логов web-сервисов:

- Перейдите в каталог сервиса, логи которого необходимо получить (keybox, keyboxservice, keyboxremote, credprovapi). Путь по умолчанию %SystemDrive%\inetpub\wwwroot\keybox. Каталог сервиса CardMonitor по умолчанию находится %ProgramFiles%/Rutoken KeyBox/CardMonitor.
- Создайте папку Logs.
- В свойствах папки на вкладке **Безопасность** (Security) выставите права на **Изменение** (Modify) для группы пользователей **IIS_IUSRS** и сервисной учетной записи для работы с центром сертификации, используемым в Вашей конфигурации. Убедитесь в том, что права применены на папку и все вложенные в неё подпапки и файлы.
- Откройте файл Web.nlog (в текстовом редакторе, например, Блокнот) и изменить параметр **minlevel="Off"** на **"Info"**: ***<logger name="*" minlevel="Info" writeTo="file" />***
- Сохраните изменения в файле.
- Воспроизвести сценарий, логи которого необходимо получить.
- Перейти в ранее созданный каталог Logs. В нем появится папка, содержащая файлы с отладочной информацией.
- Прислать каталог Logs со всем его содержимым на hotline@rutoken.ru.
- Для отключения логирования измените значение параметра **minlevel** с **"Info"** на **"Off"**.

Раздел 3. Руководство администратора системы

О системе

Назначение системы

Рутокен KeyBox предназначен для внедрения, управления и учета аппаратных средств аутентификации пользователей в масштабах предприятия. Рутокен KeyBox обеспечивает централизованное управление средствами аутентификации в течение всего жизненного цикла, учет средств аутентификации и аудит их использования, быстрое и самостоятельное решение проблем пользователей без обращения к администраторам, в том числе за пределами предприятия.

Структура системы

Система состоит из серверной и клиентской частей.
Компоненты серверной части:

- Web-сервисы:
  - Management Console — консоль администратора, позволяющая конфигурировать систему, работать с устройствами аутентификации пользователей, просматривать журнал операций системы;
  - Self Service — консоль самообслуживания, позволяющая пользователям самостоятельно работать со своими устройствами аутентификации;
  - Remote Self Service - консоль самообслуживания, позволяющая пользователям выполнять операции с устройствами аутентификации за пределами домена;

- Вспомогательные утилиты:
  - KeyBox.StorageAD.exe — мастер конфигурирования домена, создающий необходимую структуру каталогов в AD;
  - KeyBox.CertEnroll.exe — утилита для выпуска сертификата “Агент регистрации”;
  - KeyBox.KeyGen.exe — утилита для создания ключа шифрования;
  - Card Monitor.exe — служба мониторинга устройств аутентификации;
  - RutokenKeyBoxUnblock.exe — утилита для разблокировки устройств.

Компоненты клиентской части:

- Рутокен KeyBox — Middleware
  - Middleware — компонент, предоставляющий единый интерфейс остальным компонентам системы по управлению устройствами аутентификации, подключенными к рабочей станции пользователя.
- Рутокен KeyBox — Client Tools
  - Credential Provider — компонент, обеспечивающий интерактивную аутентификацию пользователя, имеющий дополнительную функциональность для разблокировки устройств и их отзыва в offline- и online-режимах;
  - RutokenKeyBoxUnblock — инструмент для offline-разблокировки устройств, которые не используются для входа в операционную систему.

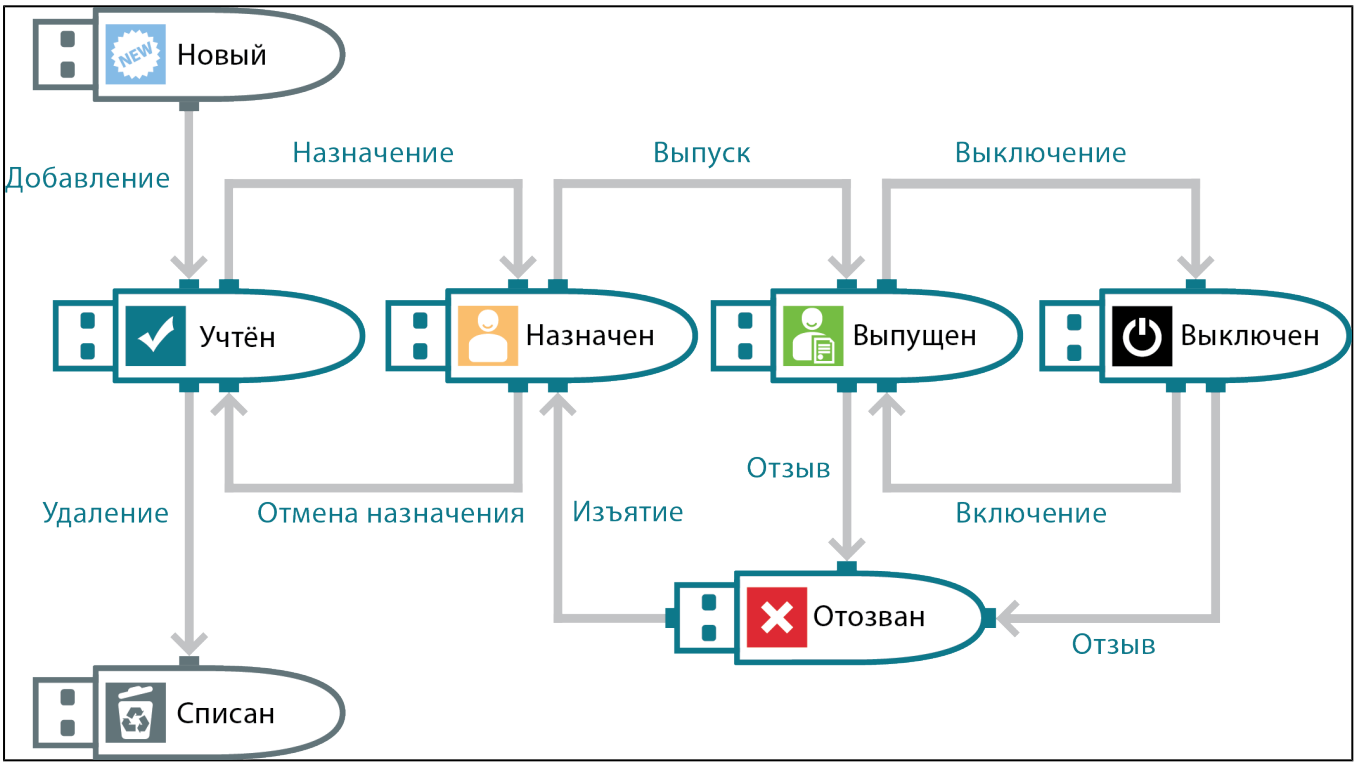
В качестве средства хранения данных и настроек системы используется Active Directory. Расширение схемы Active Directory не требуется.

Роли пользователей

В системе определены три пользовательские роли:

- Администраторы системы — обладают полными правами на управление пользователями, устройствами аутентификации, управление системой и изменение ее конфигурации.
- Операторы службы поддержки — обладают правами на управление устройствами аутентификации пользователей, без возможности изменения конфигурации системы.
- Пользователи системы — обладают правами на управление своими устройствами аутентификации.

Жизненный цикл устройства в системе



Состояние	Описание
Новый	Устройство не зарегистрировано в системе
Учтен	Устройство зарегистрировано в системе, но не привязано к пользователю
Назначен	Устройство привязано к учетной записи пользователя, но еще не готово к работе (сертификаты не выпущены)
Выпущен	Сертификаты выпущены и записаны на устройство
Выключен	Сертификаты временно отозваны
Отозван	Сертификаты отозваны без возможности восстановления
Списан	Устройство удалено из системы

Консоль администратора

Management Console — консоль администратора, позволяющая конфигурировать систему, работать с устройствами аутентификации пользователей, просматривать журнал операций системы.
Доступ к web-приложению осуществляется по URL: *https://[адрес сервера Рутокен KeyBox]/keybox/*
Работа с приложением доступна для групп:

Группа	Описание	Пользователи	Доступные разделы
Rutoken KeyBox Admins	Члены группы обладают полными правами на управление системой Рутокен KeyBox (конфигурирование	Администраторы системы	Пользователи, Устройства, Аудит, Конфигурация

Группа	Описание	Пользователи	Доступные разделы
	системы, изменение пользовательских настроек, управление устройствами идентификации).		
Rutoken KeyBox HelpDesk Operators	Члены группы обладают правами на управление устройствами идентификации	Сотрудники технической поддержки	Пользователи, Устройства, Аудит

Начало работы

Для начала работы с системой необходимо:

1. Произвести инсталляцию системы в соответствии с документом «Рутокен KeyBox. Установка и настройка.»
2. Загрузить файл с лицензией.
3. Настроить политики использования устройств идентификации.
4. Добавить необходимые типы устройств в систему.

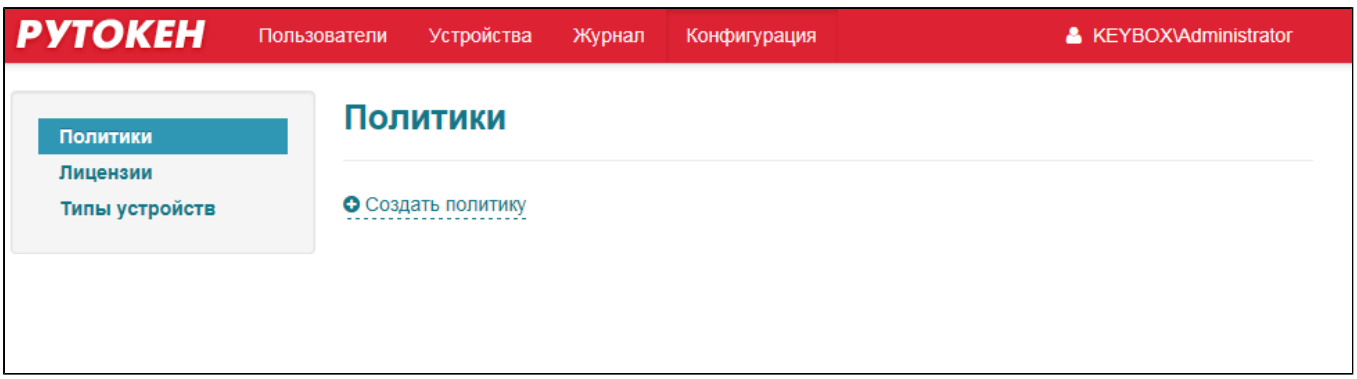
Процесс добавления лицензий и типов устройств, а также установки необходимых настроек описан в разделе Конфигурация.

Вход в систему

В зависимости от типа контроля доступа возможно два варианта аутентификации в системе:
1. Аутентификация Windows. Дополнительные действия не требуются, пройдя аутентификацию в домене пользователь получает доступ к сервисам системы.
2. Аутентификация по сертификатам. Для получения доступа к сервисам системы необходимо подключить токен с соответствующим сертификатом.

Конфигурация

Данный раздел предназначен для администраторов системы. В разделе производятся основные настройки системы: настройки параметров работы с устройствами идентификации, настройка лицензий и типов устройств аутентификации.



Лицензии

Раздел предназначен для работы с лицензиями: добавлению, обновлению. Лицензии поставляются в виде файла с расширением *.lic.

Механизм учета лицензий выглядит следующим образом: при привязке (назначении или выпуске) первого устройства аутентификации к учетной записи пользователя лицензия считается задействованной. При привязке последующих устройств новые лицензии для этой учетной записи не занимаются. Как только последнее устройство отвязывается от учетной записи пользователя, лицензия освобождается.

На странице отображено общее количество лицензий и количество занятых лицензий.

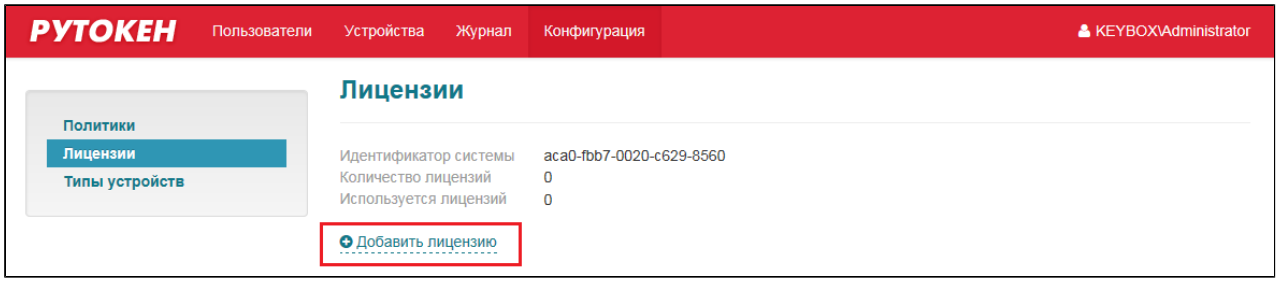
Важная информация

Лицензия предоставляется на идентификатор системы, который в свою очередь, уникален для каждого экземпляра хранилища пользователей Рутокен KeyBox. Идентификатор системы отображается в разделе *Конфигурация - Лицензии*.

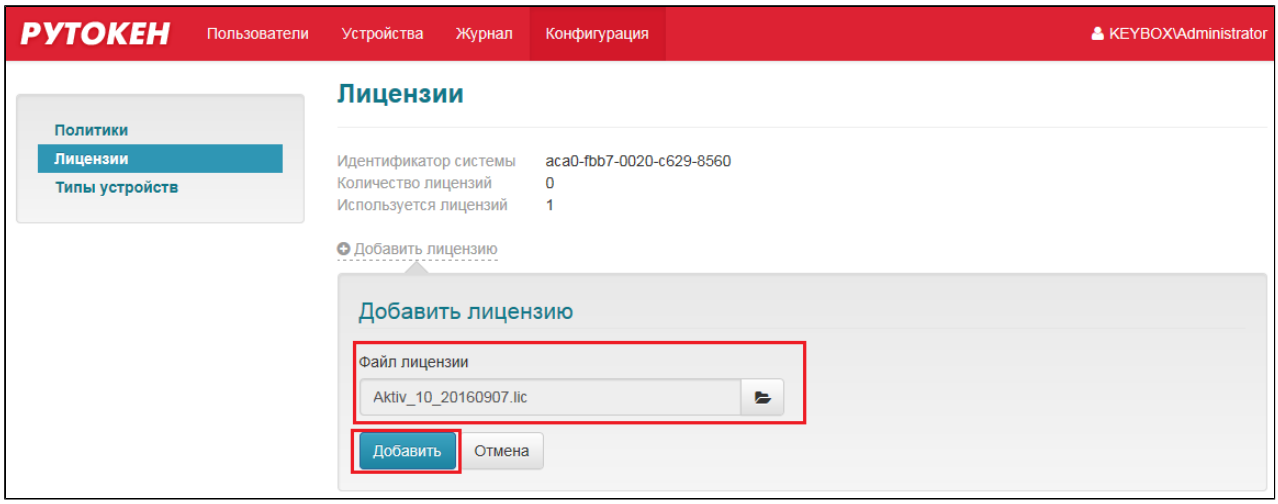
Для получения файла лицензии обратитесь в службу поддержки компании Актив, сообщив название вашей организации и идентификатор системы.

Для добавления или обновления файла лицензии:

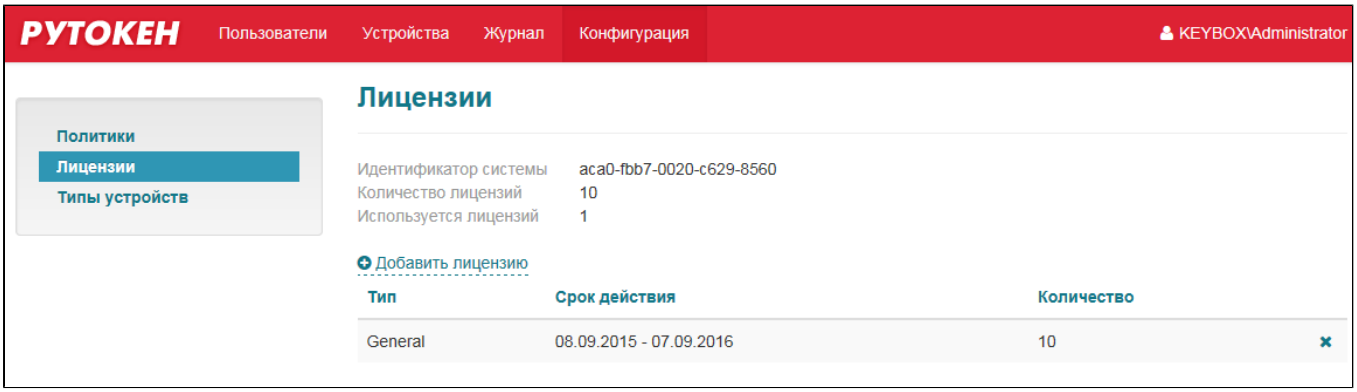
1. Перейдите в раздел Конфигурация и выберите пункт Лицензии и нажмите на ссылку **Добавить лицензию**:



2. Укажите путь к файлу лицензии и нажмите на кнопку **Добавить**:



Лицензия добавлена.

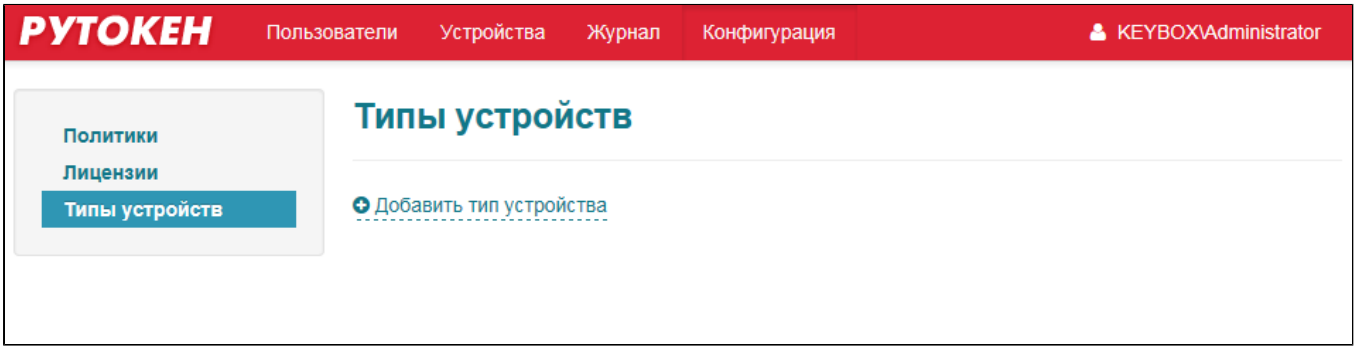


Типы устройств

Раздел предназначен для управления типами устройств, с которыми может работать система. Установленные в настройках PIN-коды используются как PIN-коды по умолчанию при работе с устройствами. PIN-код Администратора используется при добавлении устройств в систему.

В данном разделе хранится следующая информация о типе устройства:

Параметр	Назначение
Имя устройства	Название типа устройства. Совпадает с официальным названием модели. Поле является неизменяемым.
PIN-код Администратора	PIN-код Администратора устройства. Используется при добавлении устройств в систему. Если установленный в настройках PIN-код не совпадает с PIN-кодом устройства, добавление его в систему невозможно.
PIN-код Пользователя	PIN-код Пользователя устройства, установленный по умолчанию.

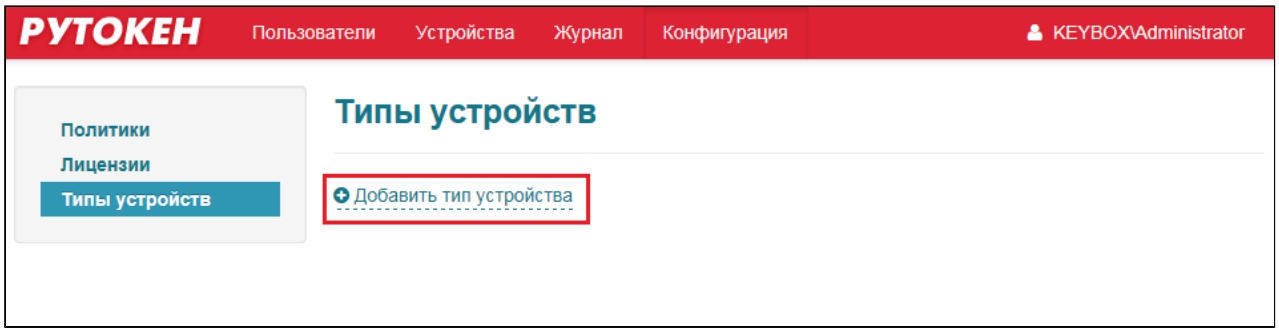


Важная информация

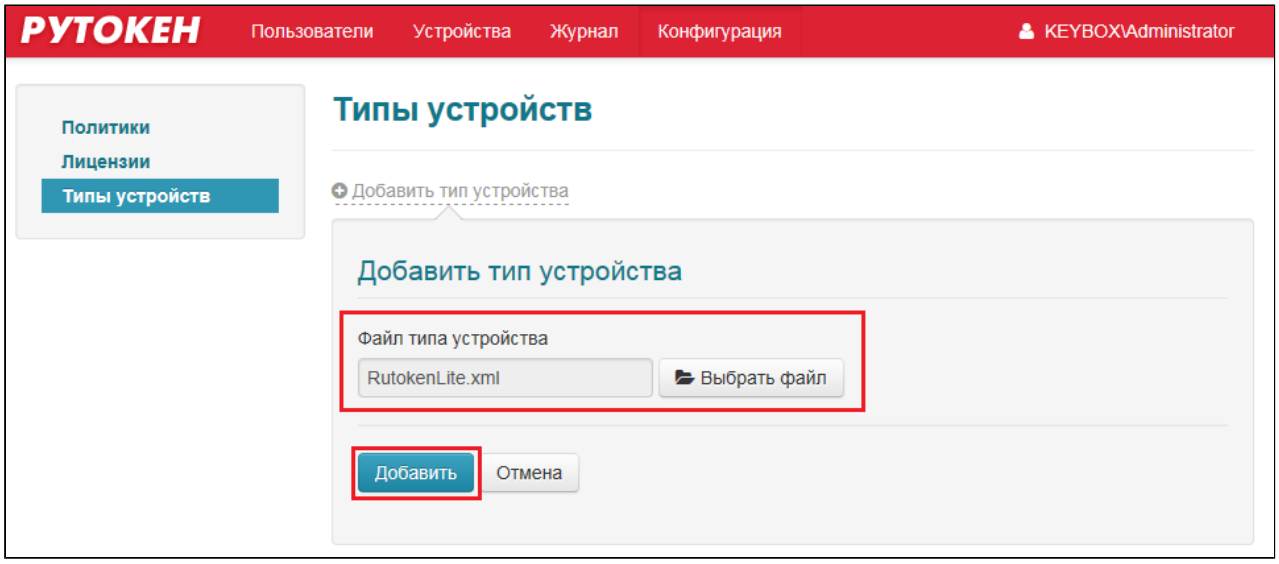
Если установленный на устройстве PIN-код Администратора не совпадает с PIN-кодом в настройках, то добавление устройства в систему невозможно.

Для работы системы с определенным типом устройства аутентификации:

1. Перейдите в раздел Конфигурация и выберите пункт **Типы устройств** и нажмите на ссылку **Добавить тип устройства**:



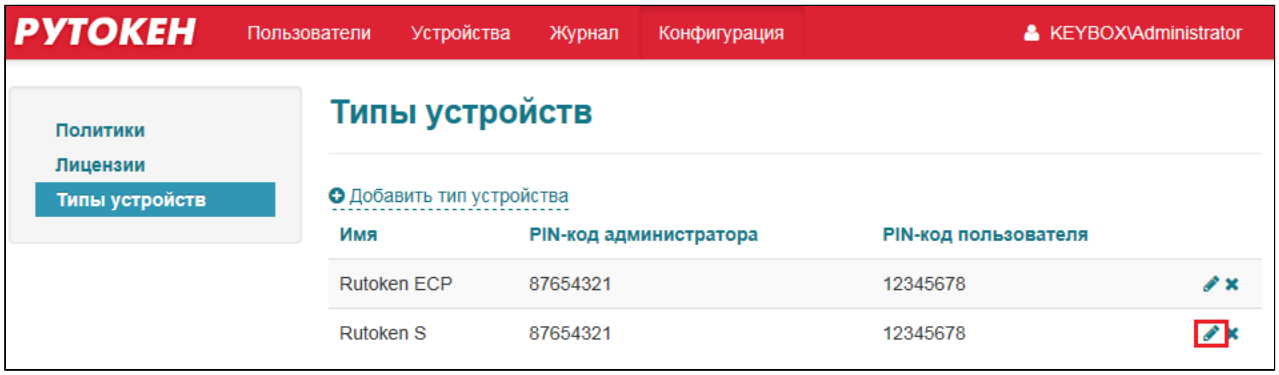
2. Укажите путь к файлу профиля типа устройств и нажмите на кнопку **Добавить**:



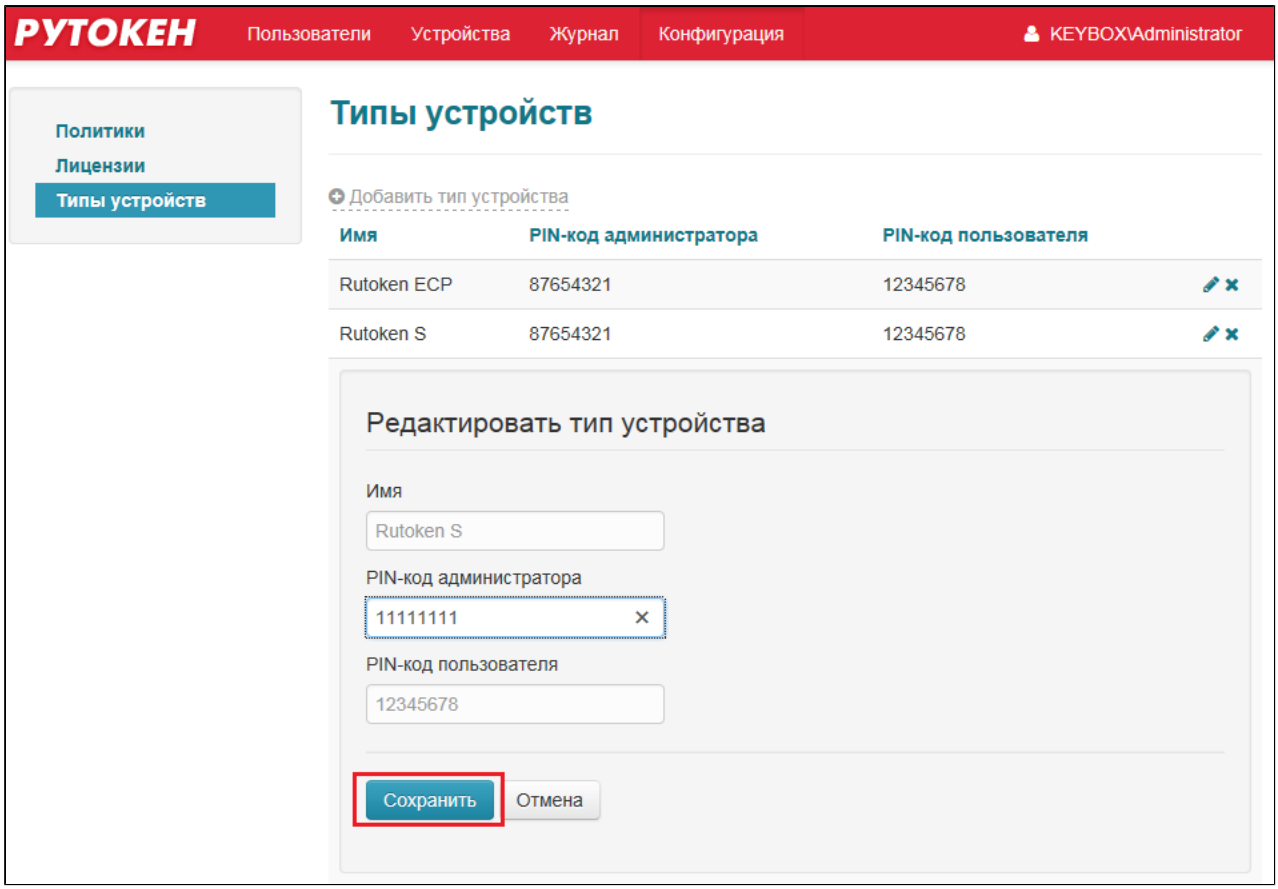
Тип устройств добавлен. Система может работать с добавленным типом устройств аутентификации.

Для изменения профиля типа устройства:

1. Перейдите в раздел Конфигурация и выберите пункт **Типы устройств** и нажмите на пиктограмму в строке типа, в профиль которого необходимо внести изменения:



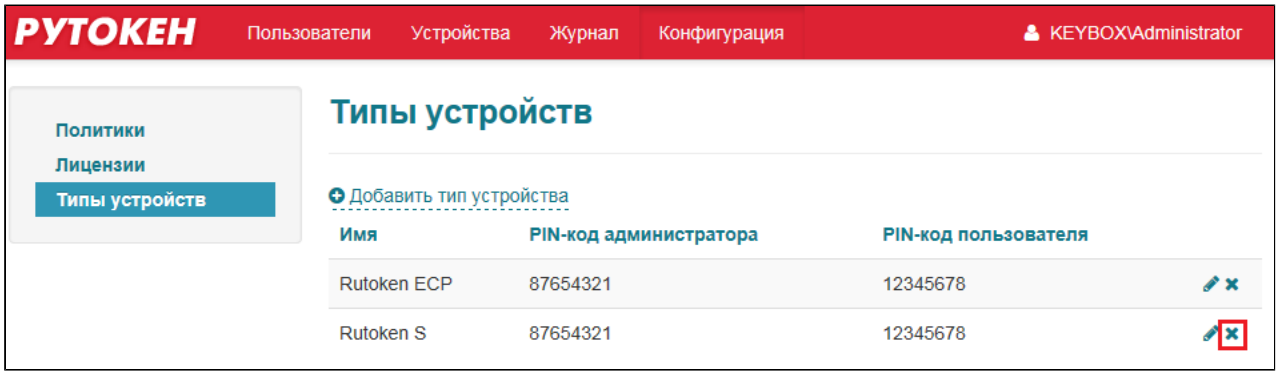
2. Внесите изменения и нажмите на кнопку **Сохранить**:



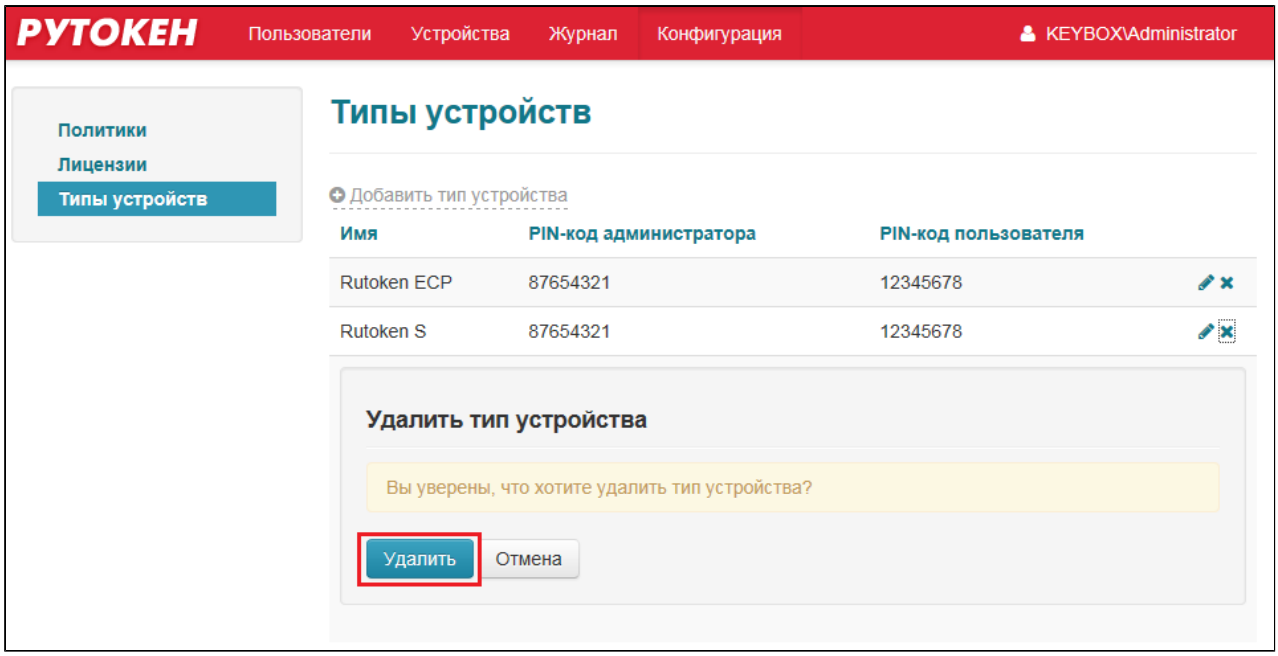
Профиль типа устройства изменен.

Если по какой-либо причине работа с определенным типом устройств больше не планируется, то можно удалить его из системы. Если в системе зарегистрированы устройства данного типа, то его удаление невозможно. Для удаления типа устройств:

1. Перейдите в раздел Конфигурация и выберите пункт Типы устройств и нажмите на пиктограмму ✖ в строке типа, который необходимо удалить:



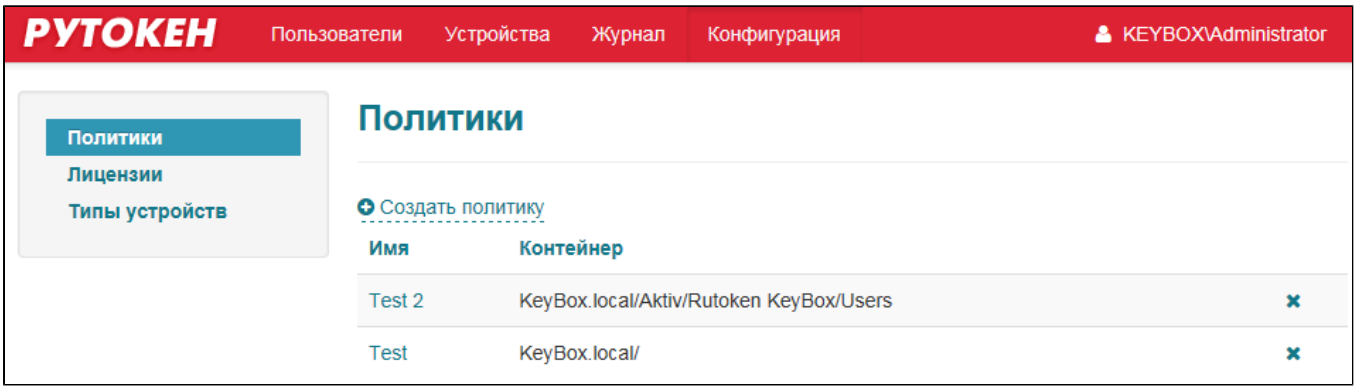
2. Подтвердите удаление:



Устройства данного типа больше не могут использоваться в системе.

Политики

В разделе Политики задаются настройки, определяющие правила работы с системой и устройствами аутентификации для пользователей. Действие политики распространяется на тот контейнер Active Directory, к которому она привязана. В системе не могут существовать политики с одинаковой областью применения. Области применения политик могут пересекаться, в данном случае если существует политика, действие которой распространяется на весь домен, и политика, действующая на определенное подразделение домена, а пользователь, для которого требуется выпустить устройство входит в это подразделение , то при выпуске политика, распространяемая на это подразделение, будет выбрана автоматически.



Политика состоит из следующих групп настроек:

Группа настроек	Описание
Общие	Сведения об имени и области действия политики
Настройки PKI Microsoft Удостоверяющие центры Шаблоны КриптоПро 1.5 Удостоверяющие центры Шаблоны КриптоПро 2.0 Удостоверяющие центры Шаблоны	Информация об используемых в системе центрах сертификации, шаблонах сертификатов и параметрах их использования в системе
Indeed EA	Параметры интеграции с системой Indeed Enterprise Authentication и Indeed Enterprise Single Sign-On
Поведение	Параметры работы пользователей с устройствами в системе
Выпуск Инициализация устройства	Параметры выпуска устройств Параметры инициализации устройства
Аутентификация Секретные вопросы	Параметры аутентификации по секретным вопросам
Уведомления Группы получателей Уведомления администратора Уведомления пользователя Шаблоны администратора Шаблоны пользователя	Настройки уведомлений, отправляемых системой автоматически по e-mail

Важная информация

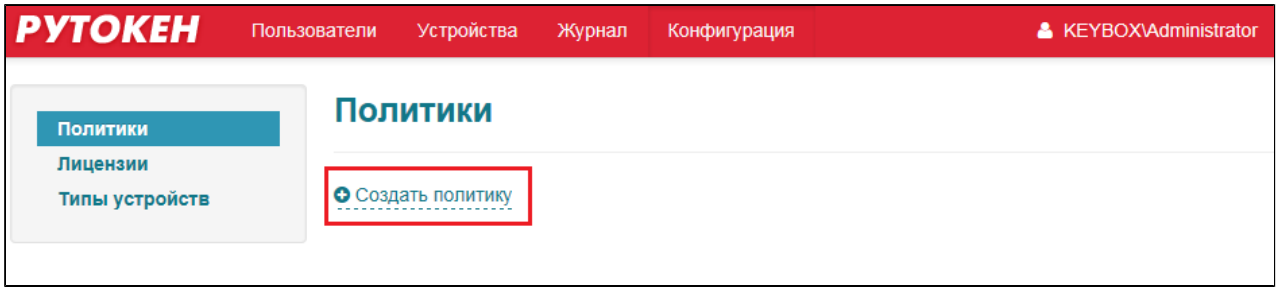
После создания политики изменить область ее применения невозможно.

Важная информация

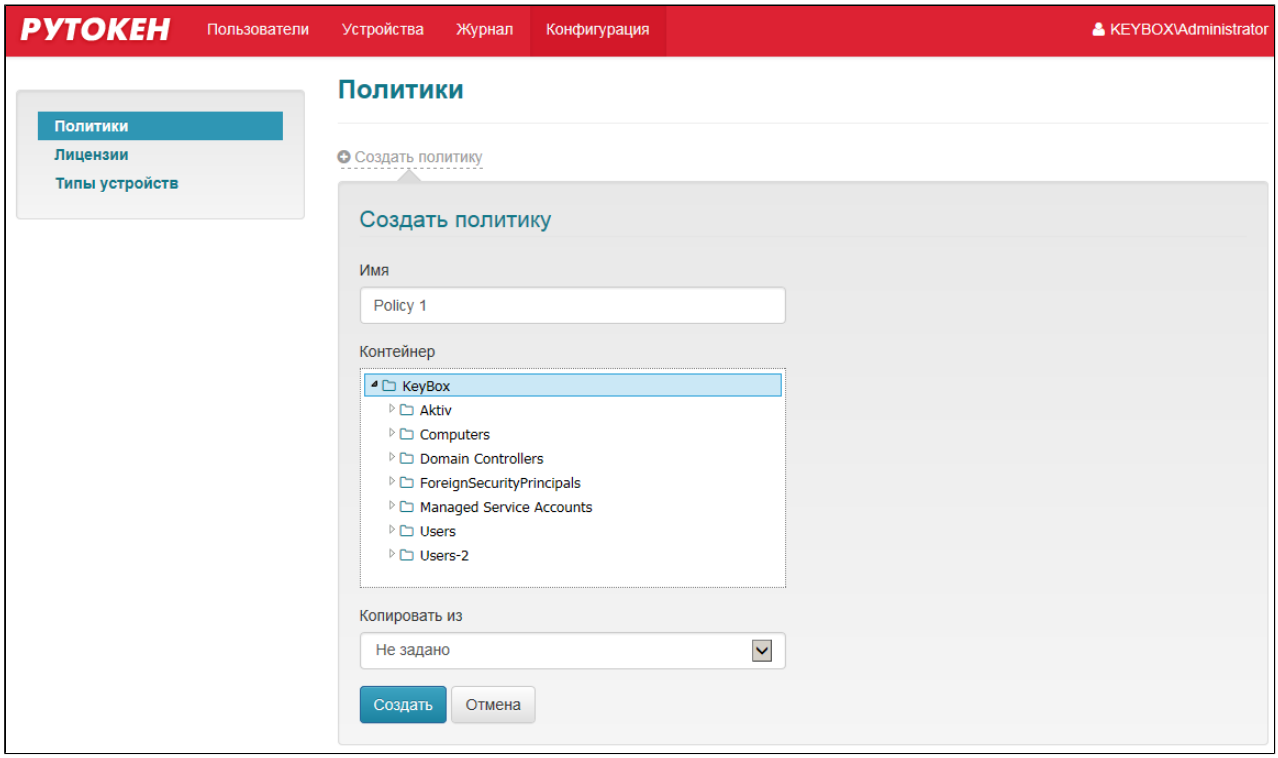
Отображение параметров того или иного удостоверяющего центра, а так же отображение параметров интеграции с системой Indeed EA определяется в файле конфигурации приложения Management Console. См. **Рутокен KeyBox.Руководство по установке и настройке**.

Для создания политики:

1. Перейдите в раздел Конфигурация и выберите пункт Политики и нажмите на ссылку **Создать политику**:



2. Укажите область применения политики и ее название и нажмите на кнопку **Создать**:



Политика создана.

Важная информация

Нельзя создать политики с одинаковой областью действия. Однако, можно создавать политики, области действия которых пересекаются.

Например, существует политика, действие которой распространяется на весь домен Windows, и политика, действующая на определенное подразделение домена.
Если пользователь, для которого требуется выпустить смарт-карту входит в подразделение, для которого определена политика, то при выпуске смарт-карты эта политика, распространяемая на это подразделение, будет выбрана автоматически.
В случае использования каталогов пользователей, расположенных в УЦ КриптоПро 1.5 и 2.0 распространение политик происходит аналогичным образом.

Чтобы удалить политику из системы, выберите её в списке и нажмите кнопку  . Подтвердите действие нажатием на кнопку Удалить. Политику можно удалить только в том случае, если она не используется (т.е. в системе нет ни одной карты, выпущенной с применением этой политики).

Если в системе создана хотя бы одна политика, то последующие можно создавать путем копирования. В результате будут скопированы все параметры, кроме названия и контейнера, на который распространяется данная политика.

Для создания политики путем копирования необходимо указать политику в выпадающем списке **Копировать из**. После этого автоматически будет осуществлен переход к ее настройкам/

Настройки PKI

Группа Настройки PKI отвечает за работу системы с центрами сертификации, использование сертификатов и их шаблонов.

Группа настроек включает в себя:

- Настройки PKI
  - Microsoft
    - Удостоверяющие центры
    - Шаблоны
  - КриптоПро 1.5
    - Удостоверяющие центры
    - Шаблоны
  - КриптоПро 2.0
    - Удостоверяющие центры
    - Шаблоны

Параметр **Импортировать сертификаты УЦ** определяет необходимость записи корневого сертификата удостоверяющего центра (или цепочки сертификатов) на устройство в момент его выпуска. Такие сертификаты не удаляются с устройства при его изъятии из системы Рутокен KeyBox. Если опция включена, то корневые сертификаты или цепочки сертификатов будут записаны на устройство. По умолчанию данная опция выключена.

Параметр **Требовать логон по смарт-карте** определяет способ входа в домен для пользователя. При установке данного флага для всех пользователей, попадающих под действие политики, будет установлен флаг в параметрах учетной записи Active Directory "Smart card is required for interactive logon" (Для интерактивного входа в сеть нужна смарт-карта). Вход в домен по логину и паролю для данного пользователя будет невозможен.

Важная информация

Запись корневого сертификата или цепочки сертификатов может не поддерживаться устройством. Уточните у производителя устройств список моделей устройств, поддерживающих данный режим.

Раздел **Microsoft** содержит параметры работы с Центрами Сертификации Microsoft.

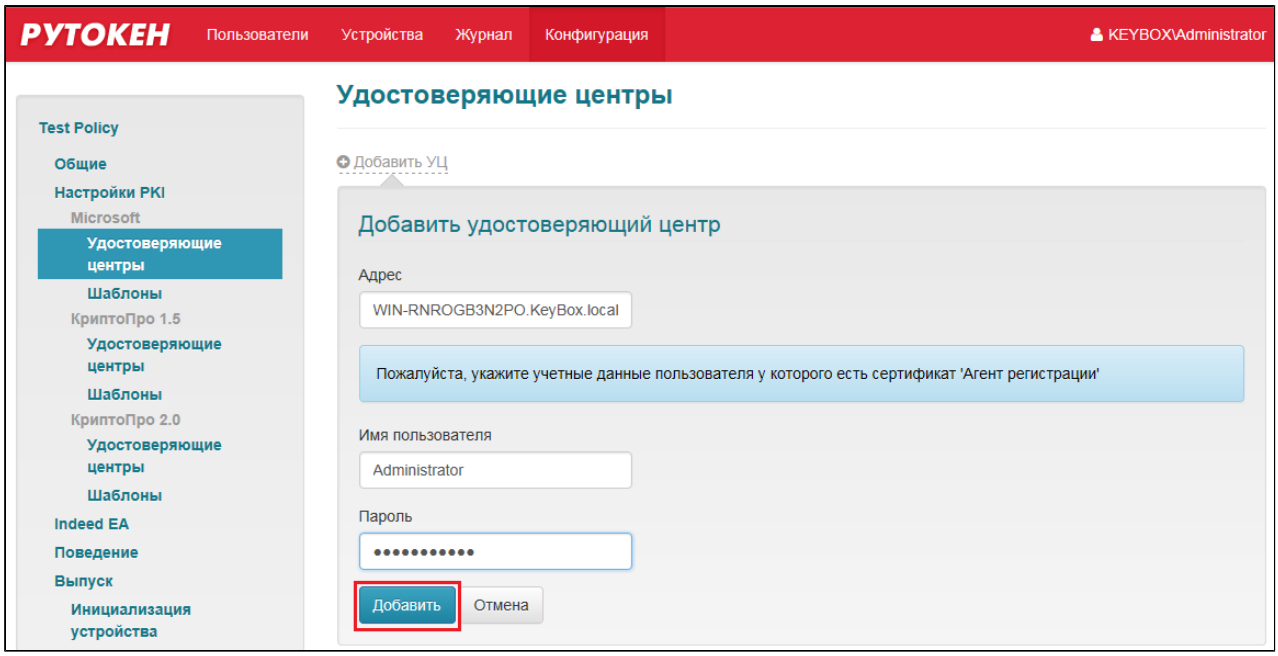
Раздел **Удостоверяющие центры** определяет удостоверяющие центры, с которыми будет работать система. Для каждого удостоверяющего центра хранится его адрес, логин и пароль пользователя, от имени которого будет производиться выпуск сертификатов в системе. Система поддерживает работу с несколькими удостоверяющими центрами в рамках одной политики.

Важная информация

Наличие пользователя с сертификатом Агент регистрации (Enrollment Agent) является обязательным условием для работы системы. От имени этого пользователя будет выполняться запрос к указанному удостоверяющему центру на выдачу сертификатов пользователям системы. Учетные данные этого пользователя могут быть изменены после добавления удостоверяющего центра в систему. См. *Настройка системы для использования с удостоверяющим центром Microsoft* в документе **Рутокен KeyBox.Руководство по установке и настройке** .

Для добавления удостоверяющего центра:

1. Откройте раздел настроек Удостоверяющие центры и нажмите на ссылку **Добавить УЦ.**
2. Введите адрес УЦ (адрес УЦ внутри домена определяется автоматически), имя пользователя и пароль учетной записи, от имени которой будут выписываться сертификаты в системе. Для этого пользователя должен быть выписан сертификат Агент регистрации. Нажмите на кнопку **Добавить**:



Удостоверяющий центр добавлен.

Важная информация

Система поддерживает одновременную работу с несколькими удостоверяющими центрами в рамках одной политики.

Для редактирования информации об удостоверяющем центре нажмите на пиктограмму  в строке удостоверяющего центра в строке записи, внесите необходимые правки и нажмите на кнопку **Сохранить.**

Для удаления удостоверяющего центра нажмите на пиктограмму  в строке удостоверяющего центра, информацию о котором нужно удалить и подтвердите удаление. Удостоверяющий центр удален из системы.

Важная информация

Нельзя удалить из системы удостоверяющий центр, на который ссылаются шаблоны политики. Для удаления такого удостоверяющего центра необходимо сначала удалить все шаблоны, связанные с ним.

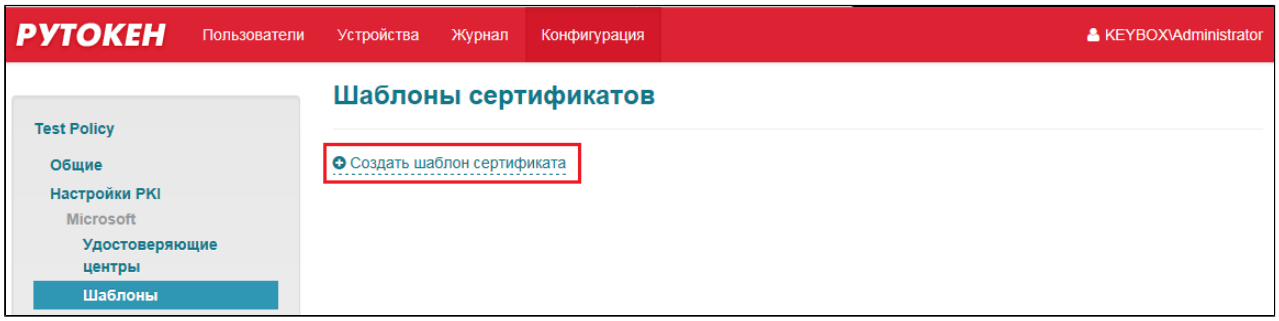
Раздел **Шаблоны** определяет, какие сертификаты будут выдаваться пользователям, попадающим под действие политики.

Важная информация

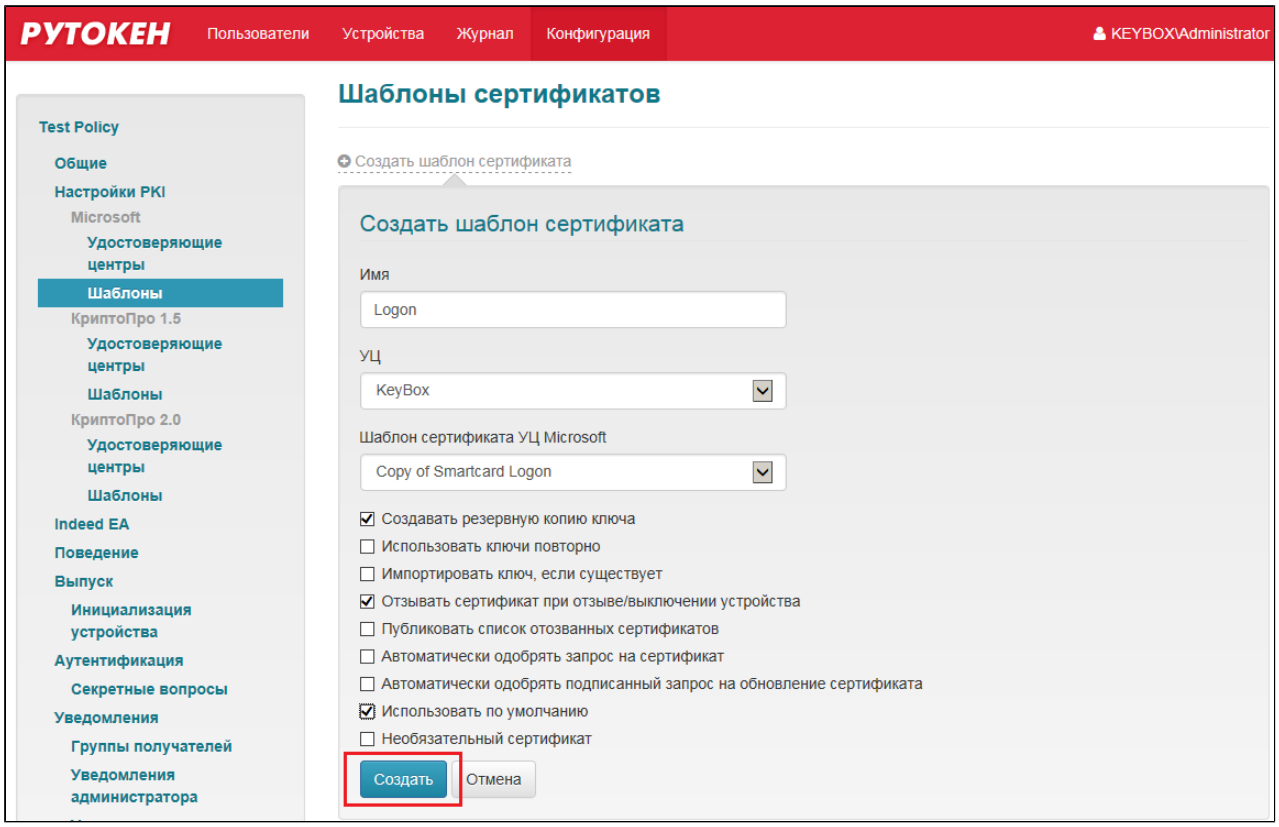
Перед созданием шаблонов в системе Рутокен KeyBox убедитесь, что необходимые шаблоны сертификатов включены в заданном центре сертификации.

Чтобы добавить шаблон выдаваемого сертификата:

1. Нажмите на ссылку **Создать шаблон сертификата**:



2. Заполните свойства шаблона и нажмите на кнопку **Создать**:



Для каждого шаблона устанавливается:

Параметр	Описание
Имя	Название шаблона.
УЦ	Удостоверяющий центр, выдающий сертификат.
Шаблон сертификата УЦ Microsoft	Название шаблона центра сертификации, выбирается из выпадающего списка. В список добавлены все доступные для выпуска шаблоны.
Создать резервную копию ключа	Если опция включена, ключи шифрования генерируются и сохраняются на сервере. В случае заменые устройства происходит запись сохраненных на сервере ключей на новое.

Параметр	Описание
Использовать ключи повторно	Если опция включена, то при обновлении сертификатов, записанных на устройство, будет использован существующий ключ шифрования.
Импортировать ключ, если существует	Если опция включена, то система будет искать существующие ключи на устройстве (для указанного пользователя, УЦ и шаблона) и использовать их. Генерация новых ключей выполняться не будет. Импорт ключа невозможен, если устройство будет проинициализировано перед выпуском.
Отзывать сертификат при отзыве /выключении устройства	Если опция включена, то сертификаты пользователя, хранящиеся на устройстве, будут отозваны при выключении или отзыве. Если опция выключена, то при выключении или отзыве устройства, сертификаты, хранящиеся на нём не будут отозваны.
Публиковать список отозванных сертификатов	Если опция включена, то при операциях включения, выключения или отзыва устройства будет производится внеочередная публикация списка отозванных сертификатов (CRL) для соответствующего центра сертификации.
Автоматически одобрять запрос на сертификат	Если опция включена, то запросы на сертификат будут автоматически одобрены. Если опция выключена, то в процессе выпуска карты необходимо будет дождаться одобрения запроса оператором удостоверяющего центра и затем продолжить выпуск (или завершить, если запрос будет отклонен).
Автоматически одобрять подписанный запрос на одобрение сертификата	Если опция включена, то запрос на обновление ранее выпущенного сертификата будет одобрен автоматически. Если опция выключена, то для обновления сертификата потребуется дождаться одобрения запроса оператором удостоверяющего центра.
Использовать по умолчанию	Если опция включена, то выпускаемый сертификат будет отмечаться как сертификат по умолчанию в памяти устройства и использоваться для входа пользователя в систему.
Необязательный сертификат	Если опция включена, то при выпуске карты появится возможность выбора сертификатов для записи на карту из числа отмеченных, как необязательные. Если опция выключена, то сертификат, выпущенный на основе такого шаблона считается обязательным для записи на карту.

Для редактирования информации о шаблоне сертификата нажмите на пиктограмму  в строке шаблона, информацию о котором нужно изменить, внесите необходимые изменения и нажмите на кнопку **Сохранить**.

Для удаления шаблона нажмите на пиктограмму  в строке шаблона, информацию о котором нужно удалить и подтвердите удаление.

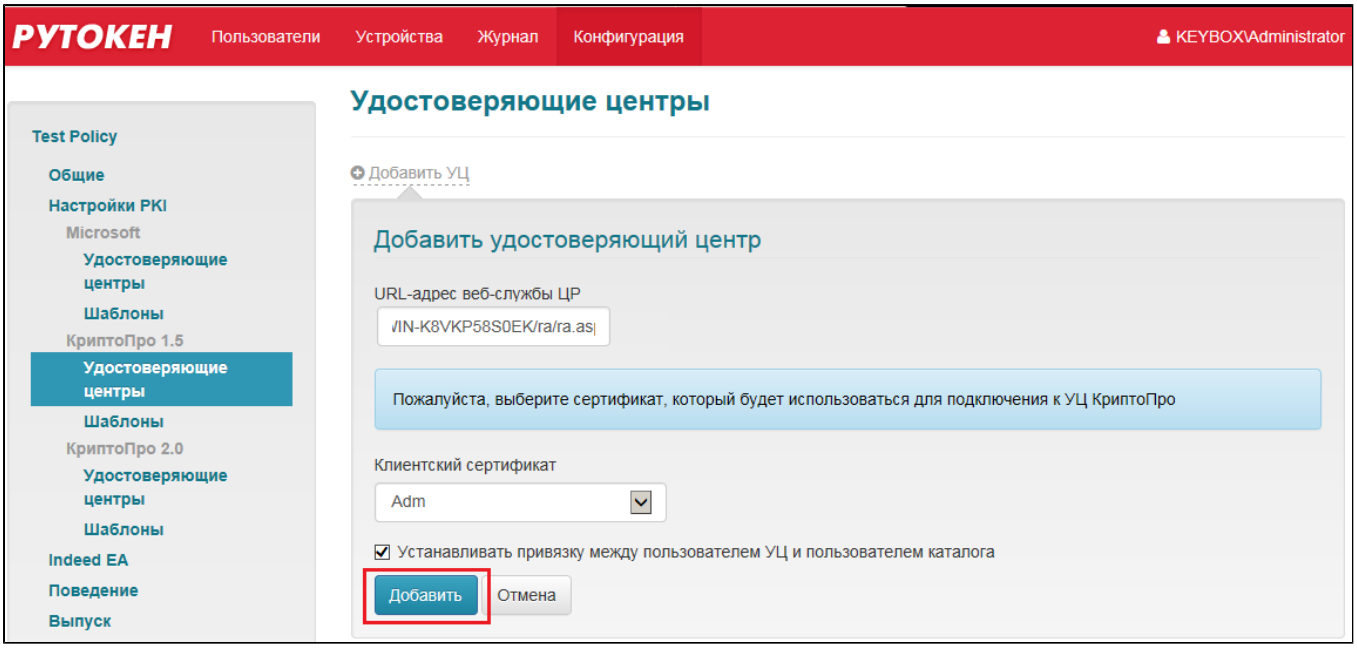
Группа настроек **КриптоПро** содержит параметры работы с Центрами Сертификации КриптоПро УЦ.

Для добавления удостоверяющего центра:

1. Откройте раздел настроек Удостоверяющие центры и нажмите на ссылку **Добавить УЦ.**
2. Введите URL веб-службы Центра Регистрации и укажите имя пользователя, обладающего сертификатом Администратора KeyBox.
   Наличие пользователя с сертификатом Выпуск сертификатов Рутокен KeyBox является обязательным условием для работы системы. От имени этого пользователя будет выполняться запрос к указанному удостоверяющему центру на выдачу сертификатов пользователям системы.

Важная информация

Система поддерживает работу с несколькими удостоверяющими центрами организации. Возможно добавление нескольких УЦ для одной политики или создание нескольких политик, указав для каждой свой удостоверяющий центр.



Для редактирования информации об удостоверяющем центре нажмите на пиктограмму в строке записи, внесите необходимые изменения и нажмите на кнопку **Сохранить**.

Для удаления удостоверяющего центра нажмите на пиктограмму в строке записи и подтвердите удаление.

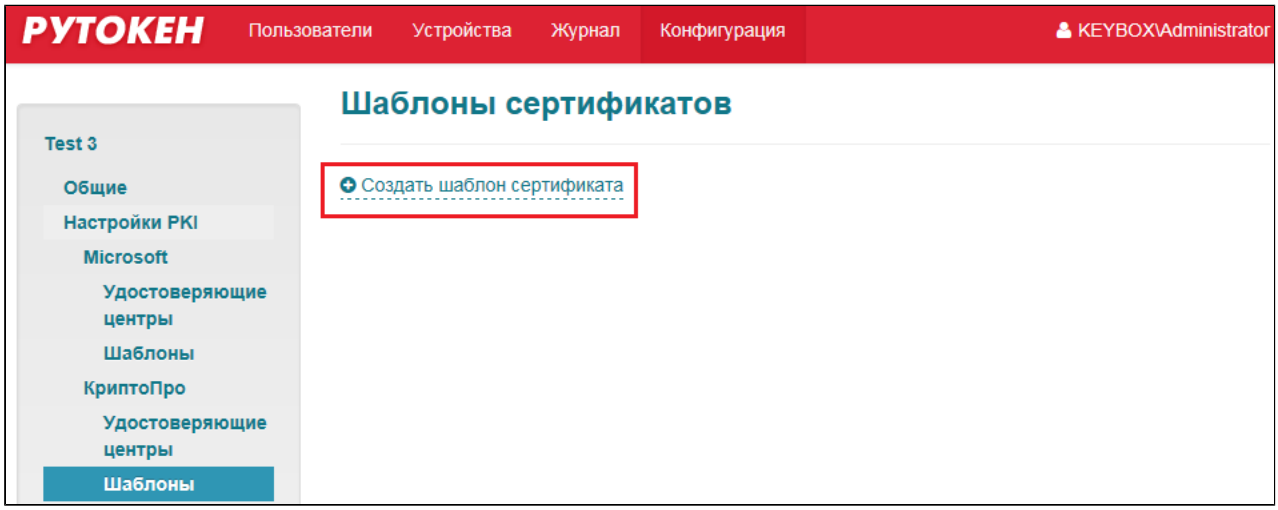
Раздел **Шаблоны** определяет, какие сертификаты будут выдаваться пользователям, попадающим под действие политики.

Важная информация

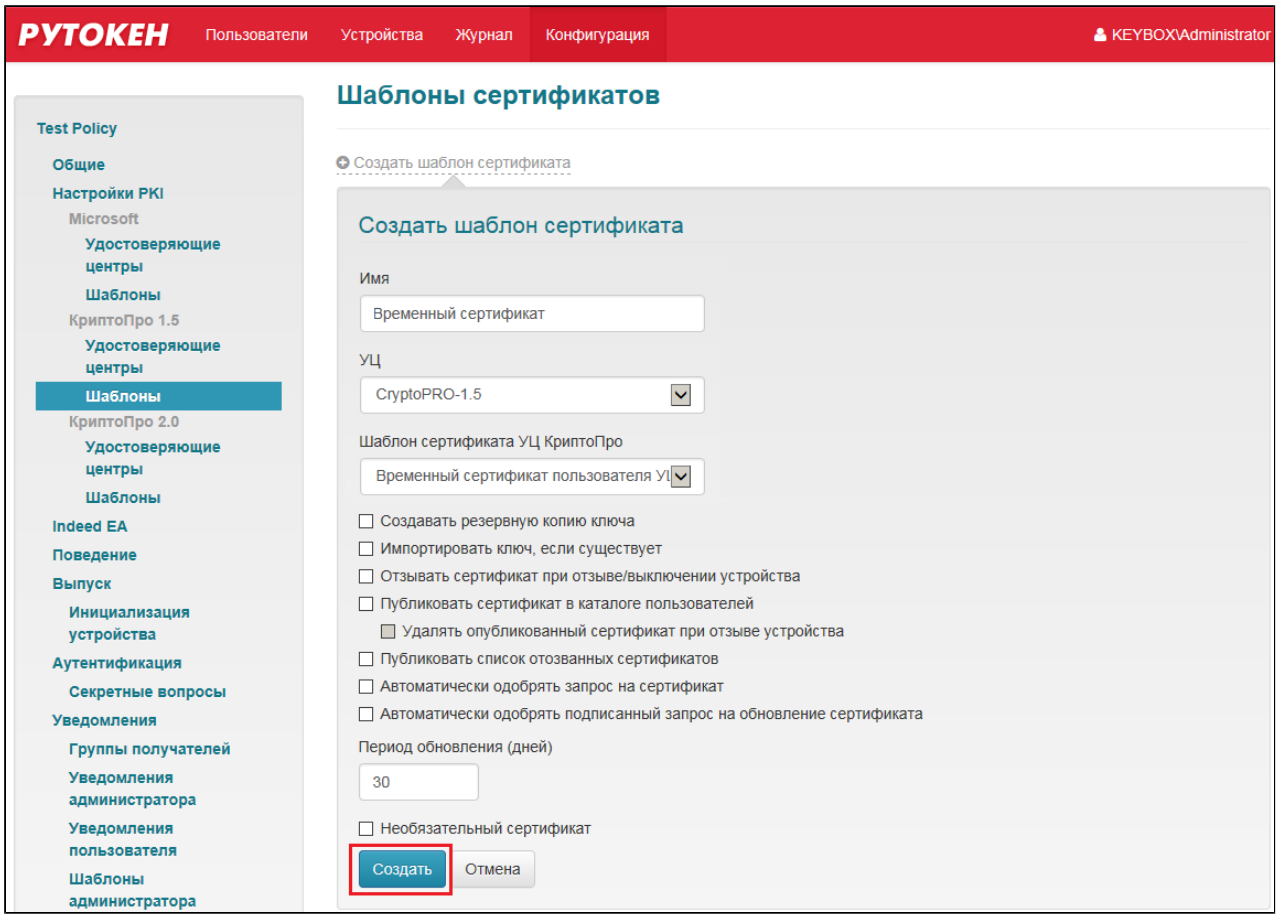
Перед созданием шаблонов в системе Рутокен KeyBox убедитесь, что необходимые шаблоны сертификатов включены в заданном центре сертификации.

Для добавления шаблона выдаваемого сертификата:

1. Нажмите на ссылку **Создать шаблон сертификата**:



2. Заполните свойства шаблона и нажмите на кнопку **Создать**:



Для каждого шаблона устанавливается:

Параметр	Описание
Имя	Название шаблона.

Параметр	Описание
УЦ	Удостоверяющий центр, выдающий сертификат.
Шаблон сертификата УЦ КриптоПро	Шаблон центра сертификации.
Создать резервную копию ключа	Если опция включена, ключи шифрования генерируются и сохраняются на сервере. В случае заменые устройства происходит запись сохраненных на сервере ключей на новое.
Импортировать ключ, если существует	Если опция включена, то система будет искать существующие ключи на устройстве (для указанного пользователя, УЦ и шаблона) и использовать их. Генерация новых ключей выполняться не будет. Импорт ключа невозможен, если устройство будет проинициализировано перед выпуском.
Отзывать сертификат при отзыве /выключении устройства	Если опция включена, то сертификаты пользователя, хранящиеся на устройстве, будут отозваны при выключении или отзыве. Если опция выключена, то при выключении или отзыве устройства, сертификаты, хранящиеся на нём не будут отозваны.
Публиковать список отозванных сертификатов	Если опция включена, то при операциях включения, выключения или отзыва устройства будет производится внеочередная публикация списка отозванных сертификатов (CRL) для соответствующего центра сертификации.
Удалять опубликованный сертификат при отзыве устройства	Если опция включена, то при отзыве устройства сертификаты, находящиеся на нем будут удалены из списка опубликованных сертификатов.
Автоматически одобрять запрос на сертификат	Если опция включена, то запросы на сертификат будут автоматически одобрены. Если опция выключена, то в процессе выпуска карты необходимо будет дождаться одобрения запроса оператором удостоверяющего центра и затем продолжить выпуск (или завершить, если запрос будет отклонен).
Автоматически одобрять подписанный запрос на одобрение сертификата	Если опция включена, то запрос на обновление ранее выпущенного сертификата будет одобрен автоматически. Если опция выключена, то для обновления сертификата потребуется дождаться одобрения запроса оператором удостоверяющего центра.
Период обновления (дней)	Позволяет задать период времени до истечения срока действия сертификата и его закрытого ключа, за который будет доступно обновление. В течение этого времени сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.
Необязательный сертификат	Если опция включена, то при выпуске карты появится возможность выбора сертификатов для записи на карту из числа отмеченных, как необязательные. Если опция выключена, то сертификат, выпущенный на основе такого шаблона считается обязательным для записи на карту

Аналогично настраивается взаимодействие с удостоверяющими центрами КриптоПро 2.0.

Indeed EA

Система Рутокен KeyBox может быть интегрирована с продуктами компании Индид – Indeed Enterprise Authentication и Indeed Enterprise Single Sign-On. Интеграция позволит объединить операции выпуска устройства (смарт-карты), запроса сертификата, записи сертификата и обучения аутентификатора в единый процесс.

Выпущенная подобным образом смарт-карта может быть использована пользователем как для аутентификации в домене и SSO-приложениях, так и для цифровой подписи или доступа к ресурсам, требующих наличие персональных сертификатов. Интеграция между системами возможна на любом этапе, независимо от того, какой из продуктов был развернут раньше.

Настройка интеграции систем Рутокен KeyBox и Indeed Enterprise Authentication состоит из двух этапов:

- Установка и настройка необходимого ПО
- Конфигурирование параметров интеграции

На **первом этапе** необходимо выполнить установку следующих компонентов:

- Indeed-Id Administration Tools на каждый сервер Рутокен KeyBox
- Indeed-Id Extended Security Provider на каждый сервер Indeed EA
- Indeed-Id SmartCard + PIN Provider на каждый сервер Indeed EA

А также выполнить настройку Extended Security Provider:

- Создать группу безопасности Indeed-ID Enrollment Admins согласно Руководству по установке и эксплуатации Indeed-Id Extended Security Provider.
- Добавить сервисную учетную запись (‘servicecm’) в группы безопасности Indeed-ID User Admins и Indeed-ID Enrollment Admins.

На **втором этапе** необходимо задать параметры интеграции в политике использования смарт-карт в Рутокен KeyBox. Перейдите в раздел **Indeed EA** в конфигурации выбранной политики и определите параметры работы с Indeed Enterprise Authentication.

Параметр	**Описание**	**Значение по умолчанию**
Включить интеграцию с Ineed EA		Выключена
Имя пользователя Пароль	Учетные данные пользователя (логин и доменный пароль), входящего в группы безопасности Indeed-ID User Admins и Indeed-ID Enrollment Admins.	Не заданы
Разрешить использование Windows logon	Если опция включена, то при выпуске смарт-карты в системе Рутокен KeyBox будет выпускаться и аутентификатор «Смарт-карта или USB-ключ + PIN»	Выключена

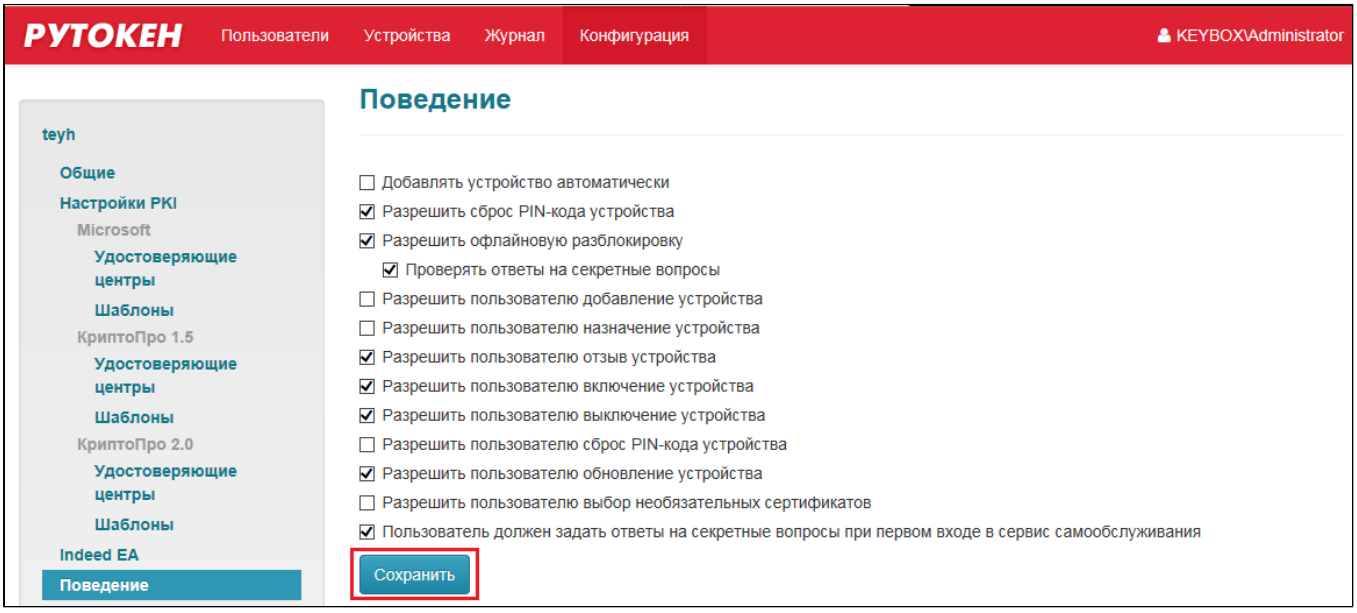
Параметр	Описание	Значение по умолчанию
	в системе Indeed Enterprise Authentication.	
Разрешить использование Enterprise SSO	Если опция включена, то при выпуске смарт-карты в системе Рутокен KeyBox пользователю будет разрешено использование технологии Indeed для аутентификации в домене при помощи компонента Indeed-Id Windows Logon.	Выключена
Генерировать случайный пароль учетной записи Windows	Если опция включена, то при выпуске смарт-карты в системе Рутокен KeyBox пользователю будет разрешено использование технологии Indeed для аутентификации в приложениях при помощи компонента Indeed-Id Enterprise SSO Agent.	Выключена

Разрешения на использование Windows Logon, Enterprise SSO и генерацию случайного пароля будут выключены в случае удаления последнего зарегистрированного аутентификатора пользователя. Например, если у пользователя не было ни одного аутентификатора в системе Indeed EA и ни одной карты в системе Рутокен KeyBox, то после выпуска смарт-карты с настроенными параметрами интеграции у пользователя появится один аутентификатор («Смарт-карта или USB-ключ + PIN») в системе Indeed EA и одна карта (например, рутокен) в системе Рутокен KeyBox.

В случае удаления карты в системе Рутокен KeyBox, удалится и аутентификатор в системе Indeed EA, а т.к. других обученных аутентификаторов нет, отключатся и разрешения на использование Indeed-Id Windows Logon, Indeed-Id Enterprise SSO и генерация случайного пароля (если хотя бы одна из этих опций была активна на момент отзыва).

Поведение

Группа настроек Поведение определяет возможные действия с устройством в рамках работы системы.



Параметр	Описание	Значение по умолчанию
Добавлять устройство автоматически	Если опция включена, то возможны выпуск и назначение устройства, которое ранее не было добавлено в систему. Если выключена, то перед тем как назначить или выпустить устройство необходимо его добавить в систему.	Выключен
Разрешить сброс PIN-кода устройства	Разрешить администратору сброс PIN-кода смарт-карты.	Включен
Разрешить офлайновую разблокировку	Позволяет разблокировать устройство пользователя в случае, когда отсутствует соединение рабочей станции пользователя с сервером Рутокен KeyBox.	Включен
Проверять ответы на секретные вопросы	Усли опция отключена, то при офлайн разблокировке не требуются ответы на секретные вопросы.	Включен
Разрешить пользователю добавление устройства	Позволяет пользователю добавление устройства в систему при его выпуске, если устройство не было добавлено администратором. Опция будет работать в случае, если включена опция "Добавлять устройство автоматически".	Выключен
Разрешить пользователю назначение устройства	Позволяет пользователю выпускать не назначенное ему устройство самостоятельно.	Выключен
Разрешить пользователю отзыв устройства	Позволяет пользователю самостоятельно отзывать устройства по причине утери или поломки. При отзыве устройства будут отозваны все сертификаты.	Включен
Разрешить пользователю выключение устройства	Позволяет пользователю самостоятельно временно выключать свои устройства. При временном выключении сертификаты пользователя будут временно отозваны до момента его включения.	Включен
Разрешить пользователю включение устройства	Позволяет пользователю самостоятельно включать устройство после временного выключения. Действие сертификатов восстанавливается.	Включен
Разрешить пользователю обновление устройства	Позволяет пользователю обновлять сертификаты самостоятельно.	Включен
Разрешить пользователю выбор необязательных сертификатов	Если опция включена, то при выпуске смарт-карты в приложении Self Service пользователь сможет выбрать (среди необязательных сертификатов), те сертификаты, которые необходимо записать на карту. Если опция выключена, то сертификаты, отмеченные в политике выпуска смарт-карт, как необязательные, записаны на карту не будут.	

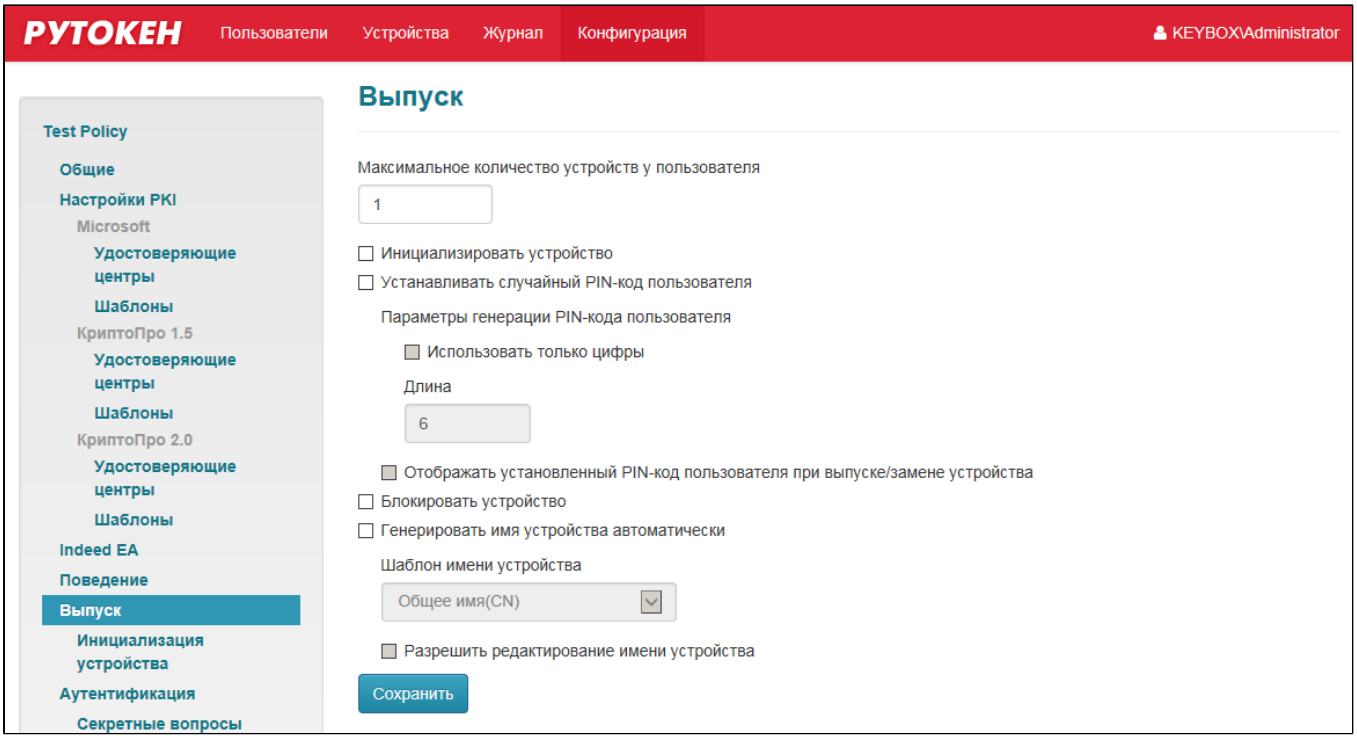
Параметр	Описание	Значение по умолчанию
Пользователь должен задать ответы на секретные вопросы при первом входе в сервис самообслуживания	Если опция включена, то при первом входе в личный кабинет пользователя он должен задать ответы на секретные вопросы.	Включен

Важная информация

Опции **Разрешить офлайновую разблокировку** и **Разрешить пользователю сброс PIN-кода устройства** будут доступны только в случае, если устройство было отформатировано со значением настройки **PIN-код Пользователя может быть изменен** соответствующим **Пользователем и Администратором**.

Выпуск

Группа настроек **Выпуск** определяет параметры выпуска устройств пользователя.



Параметр	Описание
	Определяет максимальное количество устройств, которые могут быть назначены пользователю

Параметр	Описание
Максимальное количество устройств у пользователя	
Инициализировать устройство	Если параметр включен, то в процессе выпуска будет производиться инициализация устройства, в процессе которой все данные на устройстве будут удалены без возможности восстановления
Устанавливать случайный PIN-код пользователя	Если опция включена, то в процессе выпуска смарт-карты PIN-код пользователя будет изменен на случайный. Случайный PIN-код может состоять из следующих символов: латинские строчные, латинские прописные, цифры.
Параметры генерации PIN-кода пользователя: Использовать только цифры Длина Отображать установленный PIN-код Пользователя при выпуске/замене устройства	**Параметры генерации PIN-кода пользователя**: ■ Использовать только цифры ■ Длина (от 4 до 31 символа) ■ Отображать установленный PIN-код пользователя при выпуске/замене карты Формируемый случайный PIN-код соответствует следующим правилам: ■ Содержит латинские строчные буквы ■ Содержит латинские прописные буквы ■ Содержит цифры ■ Повторы любых символов запрещены Случайный PIN-код пользователя может быть известен сотруднику, выпускающему карту. Случайный PIN-код пользователя может быть сообщен пользователю или его руководителю посредством почтового уведомления (см. **Уведомления**). Длина случайного PIN-кода зависит от настройки *Минимальная длина PIN-кода пользователя* в разделе **Инициализация карты**. Если в разделах Выпуск и Инициализация карты будут указаны разные значения длины PIN-кода пользователя, то в процессе выпуска карты будет использовано большее из них.
Блокировать устройство	Если параметр включен, то при выпуске устройства PIN-код Пользователя будет заблокирован. При получении такого устройства пользователю необходимо будет его разблокировать любым доступным способом
Генерировать имя устройства автоматически: Шаблон имени Разрешить редактирование имени устройства	Если опция включена, то в качестве имени карты может быть использовано одно из следующих значений из свойств пользователя: •Общее имя (CN) •Логин •Фамилия •E-mail •Подразделение Выбранное значение будет автоматически подставлено в имя карты в окне выпуска. При включенной опции **Разрешить редактирование имени карты** подставленное

Параметр	Описание
	имя может быть изменено сотрудником или пользователем перед выпуском карты.

Установите необходимые параметры инициализации и нажмите на кнопку **Сохранить**.

Группа настроек **Инициализация устройства** определяет параметры инициализации. Инициализация устройства производится при его выпуске, если в политике предусмотрена данная опция (группа настроек **Выпуск**).

Параметр	Описание
PIN-код Пользователя	PIN-код Пользователя, который устанавливается при инициализации. Если оставить поле пустым, то при инициализации будет установлен PIN-код Пользователя, заданный поставщиком устройства при выпуске
Максимальное количество попыток ввода PIN-кода	Определяет количество попыток ввода PIN-кода
Минимальная длина PIN-кода пользователя	Определяет минимальную длину PIN-кода Пользователя. При смене PIN-кода пользователь не может установить PIN с меньшей длиной.

Установите необходимые параметры инициализации и нажмите на кнопку **Сохранить**.

Аутентификация

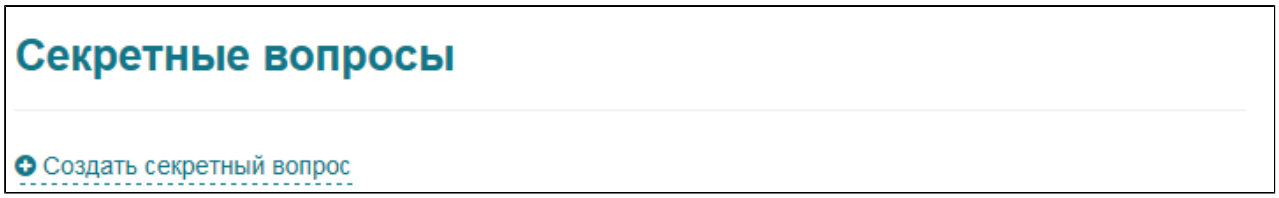
Группа настроек **Аутентификация** определяет настройки аутентификации пользователя в Remote Self-Service, а также аутентификации при выполнении операции выпуска устройств и офлайновой разблокировке.

Параметр	Описание
Количество вопросов при аутентификации	Параметр определяет количество секретных вопросов, которые будут заданы пользователю при аутентификации
Максимальное количество попыток аутентификации	Параметр определяет количество попыток ответа на секретные вопросы при аутентификации

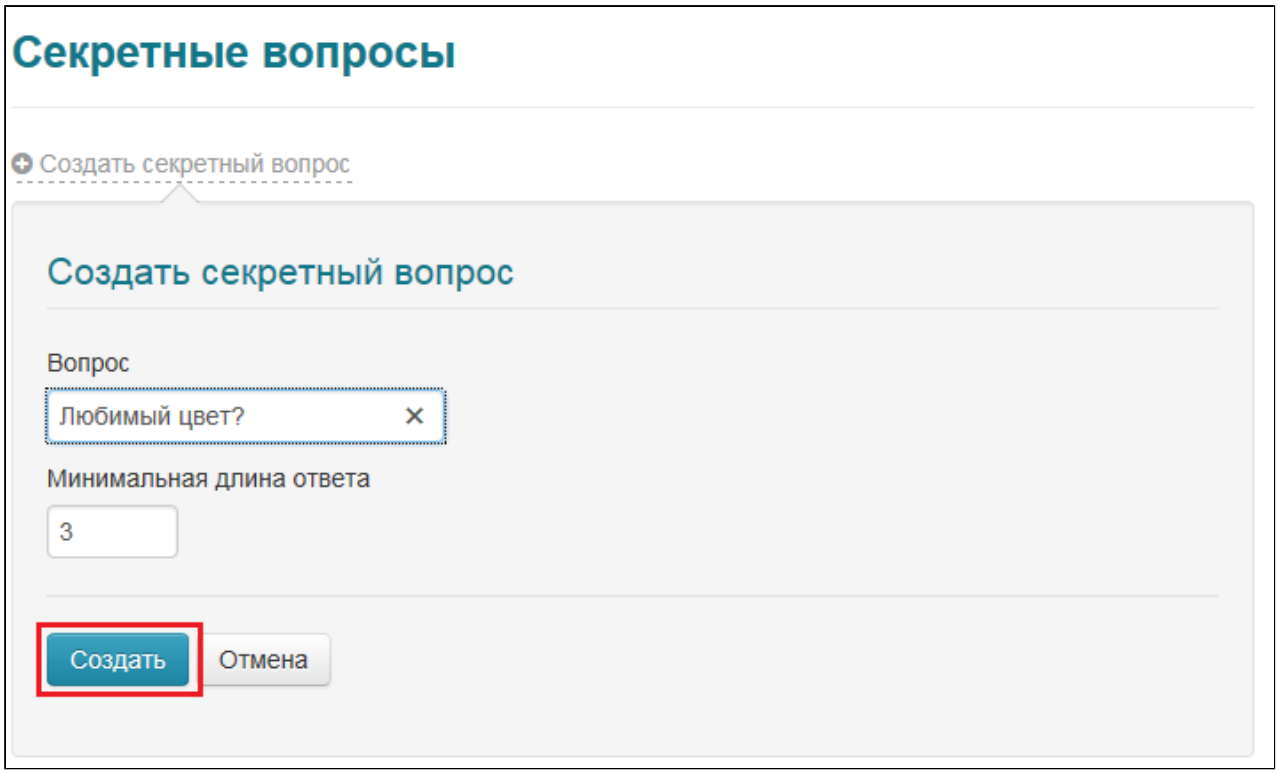
Группа настроек **Секретные вопросы** определяет, какие секретные вопросы будут предоставлены пользователю на выбор и какова минимальная длинна ответа на вопрос.

Для добавления секретного вопроса:

1. Нажмите на ссылку **Создать секретный вопрос**:



2. Введите вопрос, укажите минимальную длину ответа на него и нажмите на кнопку **Создать**:



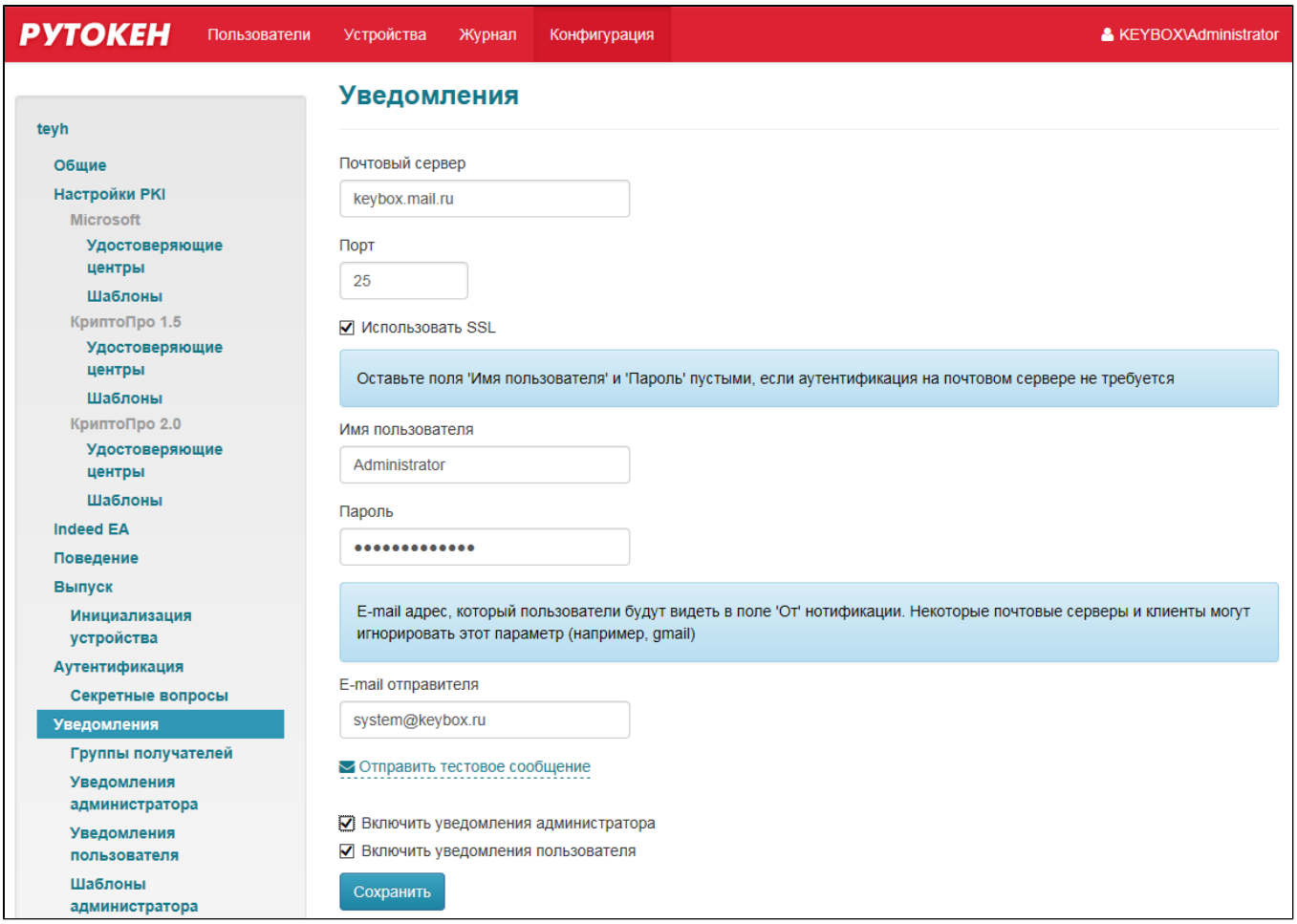
Для редактирования информации о вопросе нажмите на пиктограмму в строке вопроса, информацию о котором нужно изменить, внесите необходимые изменения и нажмите на кнопку **Сохранить**.

Для удаления удостоверяющего центра нажмите на пиктограмму в строке вопроса, информацию о котором нужно удалить, и подтвердите удаление.

Уведомления

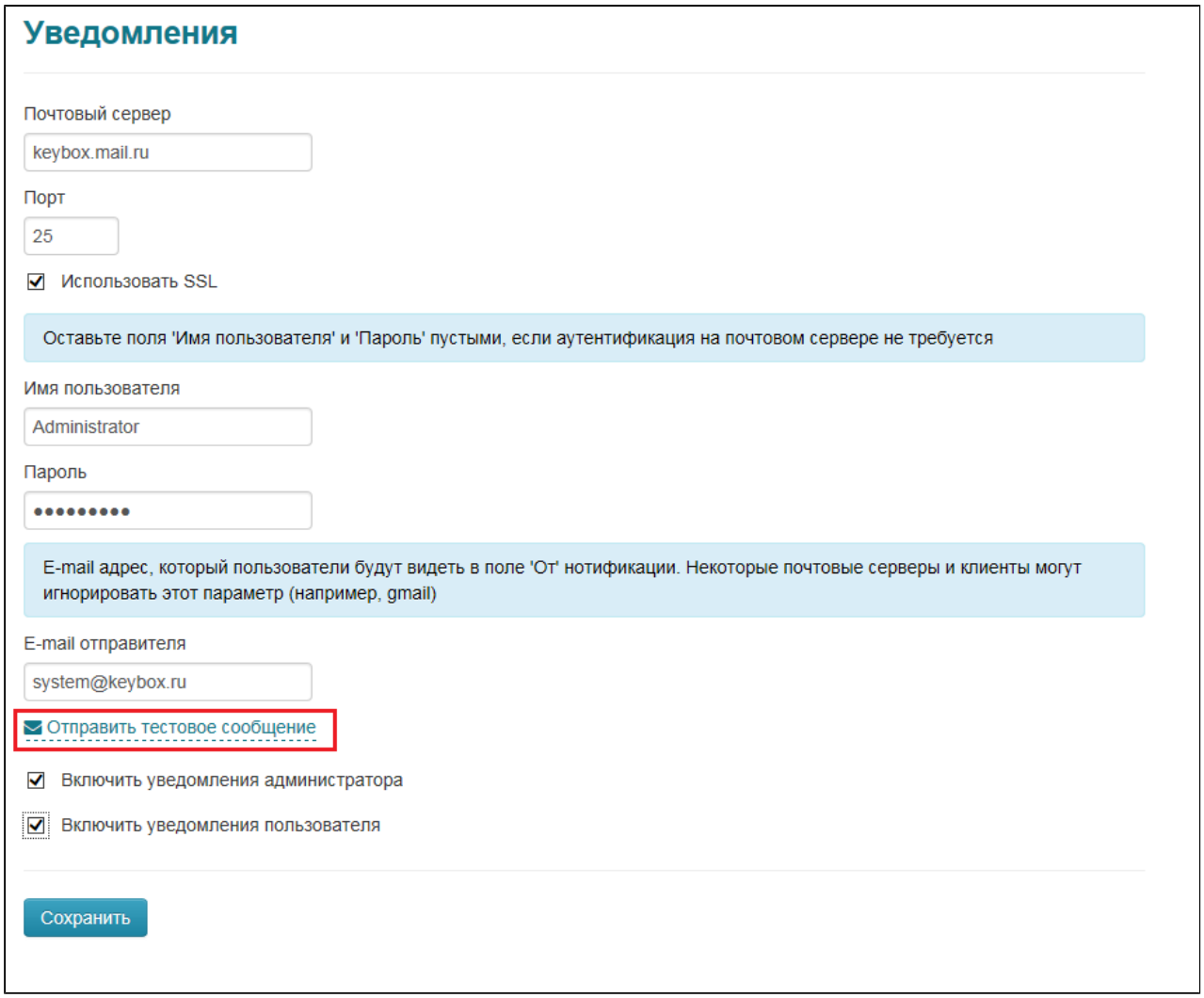
Группа настроек **Уведомления** позволяет настраивать отправку уведомлений на e-mail пользователя или администратора при наступлении определенных событий.

Для отправки уведомлений необходимо выполнить настройку почтового сервера, указав необходимые параметры:

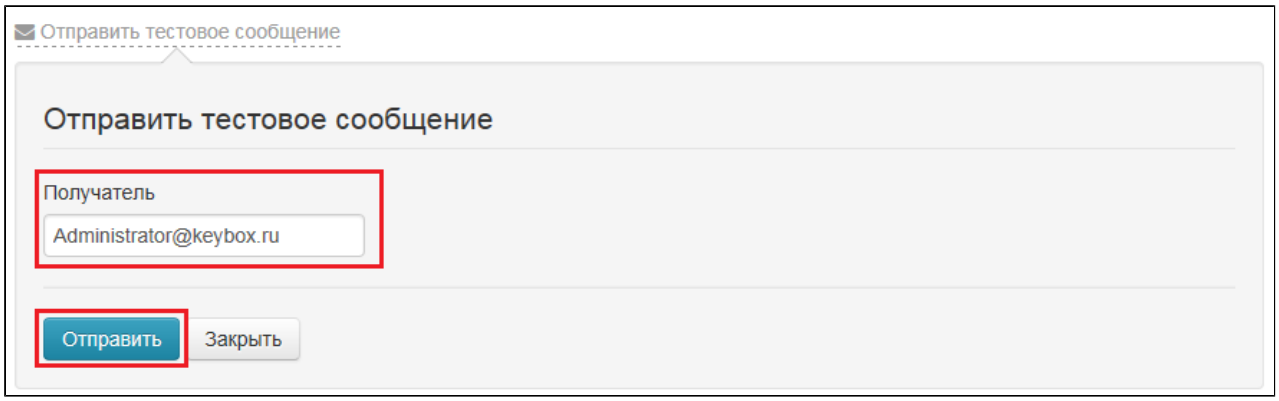


Для проверки правильности указанных параметров реализована функция отправки тестового сообщения. Чтобы отправить тестовое сообщение:

1. Нажмите на ссылку **Отправить тестовое сообщение**:



2. Введите e-mail получателя и нажмите на кнопку **Отправить**:

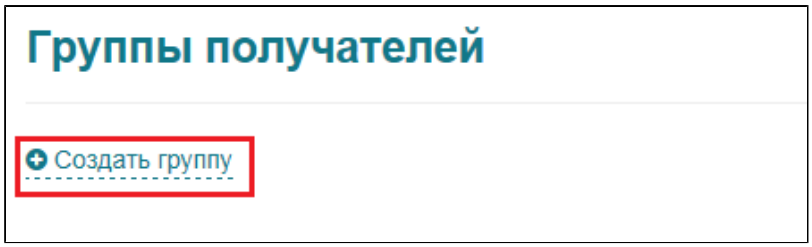


Если сообщение не было доставлено, проверьте правильность настроек почтового сервера.

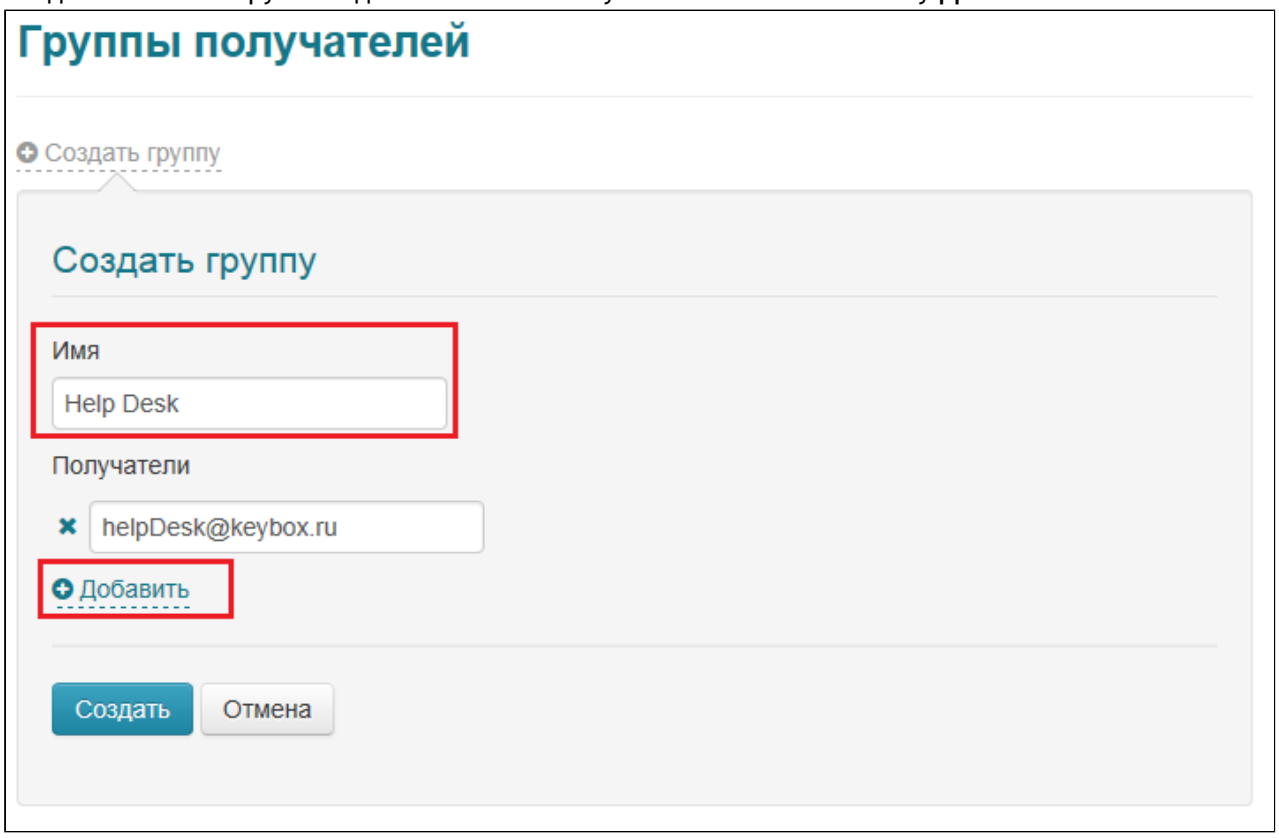
Раздел **Группы получателей** позволяет создавать группы пользователей для отправки уведомлений раздела **Уведомления администратора**. В данную группу могут быть включены администраторы системы, а так же сотрудники технической поддержки.

Для создания группы получателей:

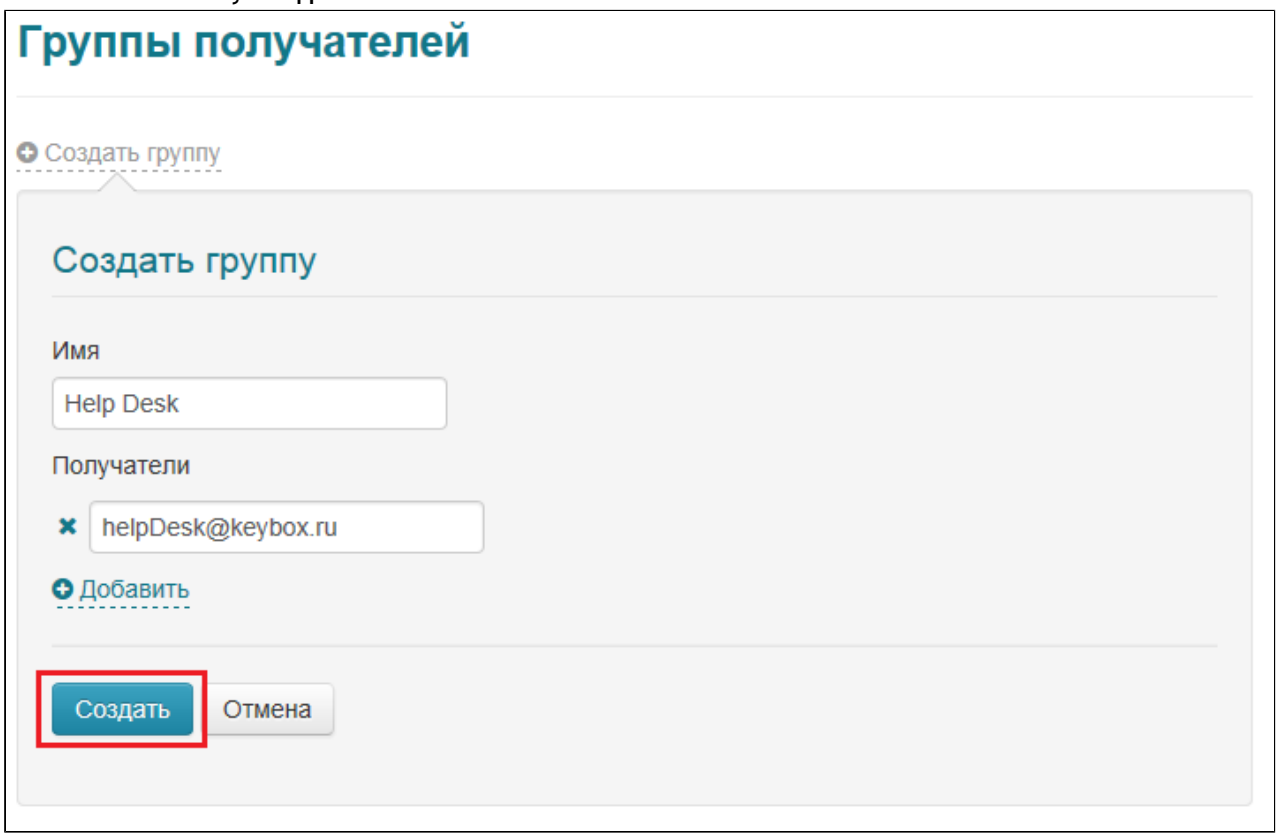
1. Нажмите на ссылку **Создать группу**:



2. Введите Название группы и добавьте e-mail получателей нажав на ссылку **Добавить**:



3. Нажмите на кнопку **Создать**:



Группа настроек **Уведомления администратора** позволяет выбрать события, уведомления о которых необходимо направлять администратору или сотруднику технической поддержки.

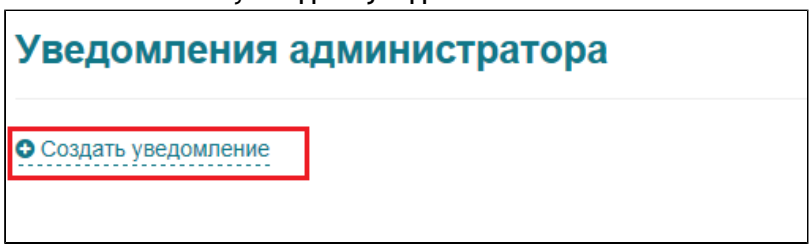
Система может оповещать о следующих типах событий:

1	Назначение устройства
2	Отвязка устройства
3	Выпуск устройства
4	Включение устройства
5	Выключение устройства
6	Отзыв устройства
7	Обновление устройства
8	Замена устройства
9	Очистка устройства
10	Сброс PIN-кода
11	Разблокировка устройства
12	Изменение PIN-кода
13	Выпуск устройства ожидает решения
14	Обновление устройства ожидает решения
15	Замена устройства ожидает решения
16	Отмена обновления устройства
17	Одобрение выпуска устройства
18	Отклонение выпуска устройства
19	Одобрение обновления устройства
20	Отклонение обновления устройства
21	Одобрение замены устройства
22	Отклонение замены устройства
23	Истечение срока действия сертификатов на устройстве
24	Изменение секретных вопросов
25	Аутентификация
26	Блокировка пользователя
27	Разблокировка пользователя

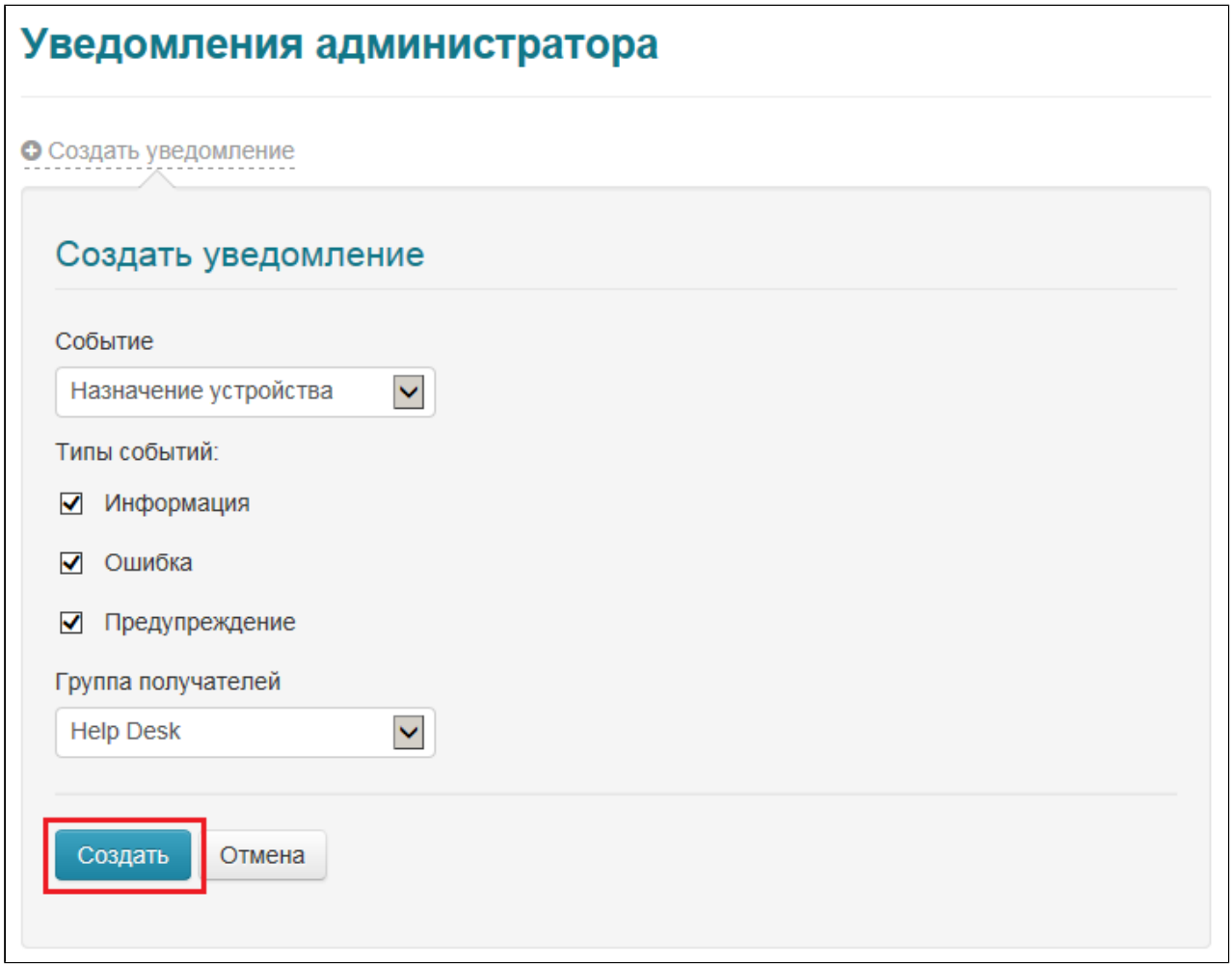
28	Сброс ответов на секретные вопросы
29	Изменение политики использования устройств

Для настройки отправки уведомления о событии:

1. Нажмите на ссылку **Создать уведомление**:



2. Выберите событие, уведомление о котором необходимо отправить, выберите типы событий, о которых необходимо уведомлять, установив соответствующие флаги, укажите группу получателей, которым необходимо отправлять уведомление и нажмите на кнопку **Создать**:



Для редактирования информации об уведомлении нажмите на пиктограмму , внесите необходимые изменения и нажмите на кнопку **Сохранить**.

Для удаления удостоверяющего центра нажмите на пиктограмму в строке уведомления, информацию о котором нужно удалить, и подтвердите удаление.

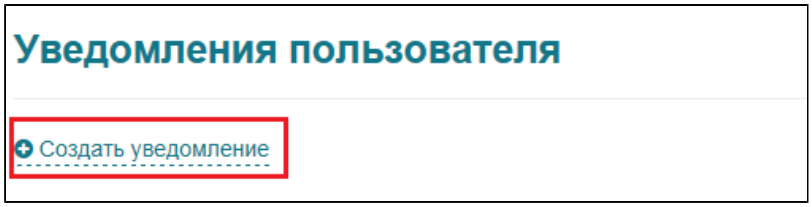
Группа настроек **Уведомления** пользователя позволяет задать события, уведомления о которых необходимо направлять пользователям системы, на которых распространяется действие политики.

Доступны уведомления о следующих событиях:

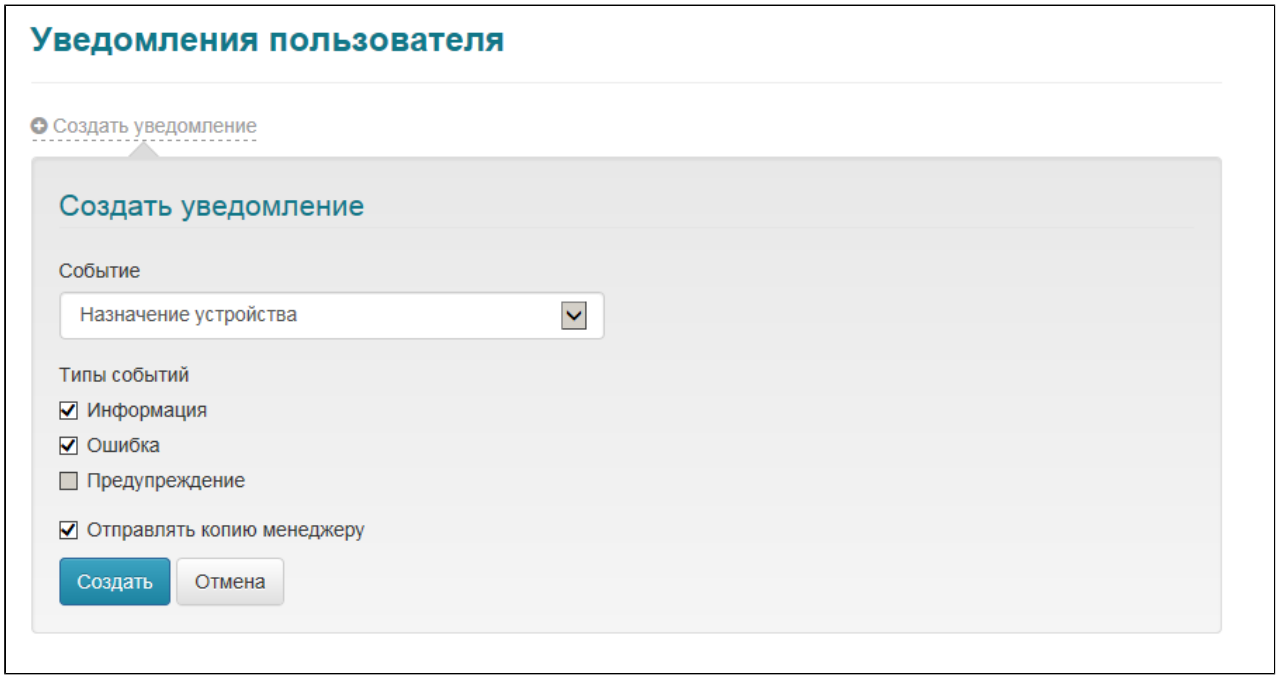
1	Назначение устройства
2	Отвязка устройства
3	Выпуск устройства
4	Включение устройства
5	Выключение устройства
6	Отзыв устройства
7	Обновление устройства
8	Замена устройства
9	Очистка устройства
10	Сброс PIN-кода
11	Разблокировка устройства
12	Изменение PIN-кода
13	Выпуск устройства ожидает решения
14	Обновление устройства ожидает решения
15	Замена устройства ожидает решения
16	Отмена обновления устройства
17	Одобрение выпуска устройства
18	Отклонение выпуска устройства
19	Одобрение обновления устройства
20	Отклонение обновления устройства
21	Одобрение замены устройства
22	Отклонение замены устройства
23	Истечение срока действия сертификатов на устройстве
24	Изменение ответов на секретные вопросы
25	Аутентификация
26	Блокировка пользователя
27	Разблокировка пользователя
28	Сброс ответов на секретные вопросы

Для настройки отправки уведомления о событии:

1. Нажмите на ссылку **Создать уведомление**:



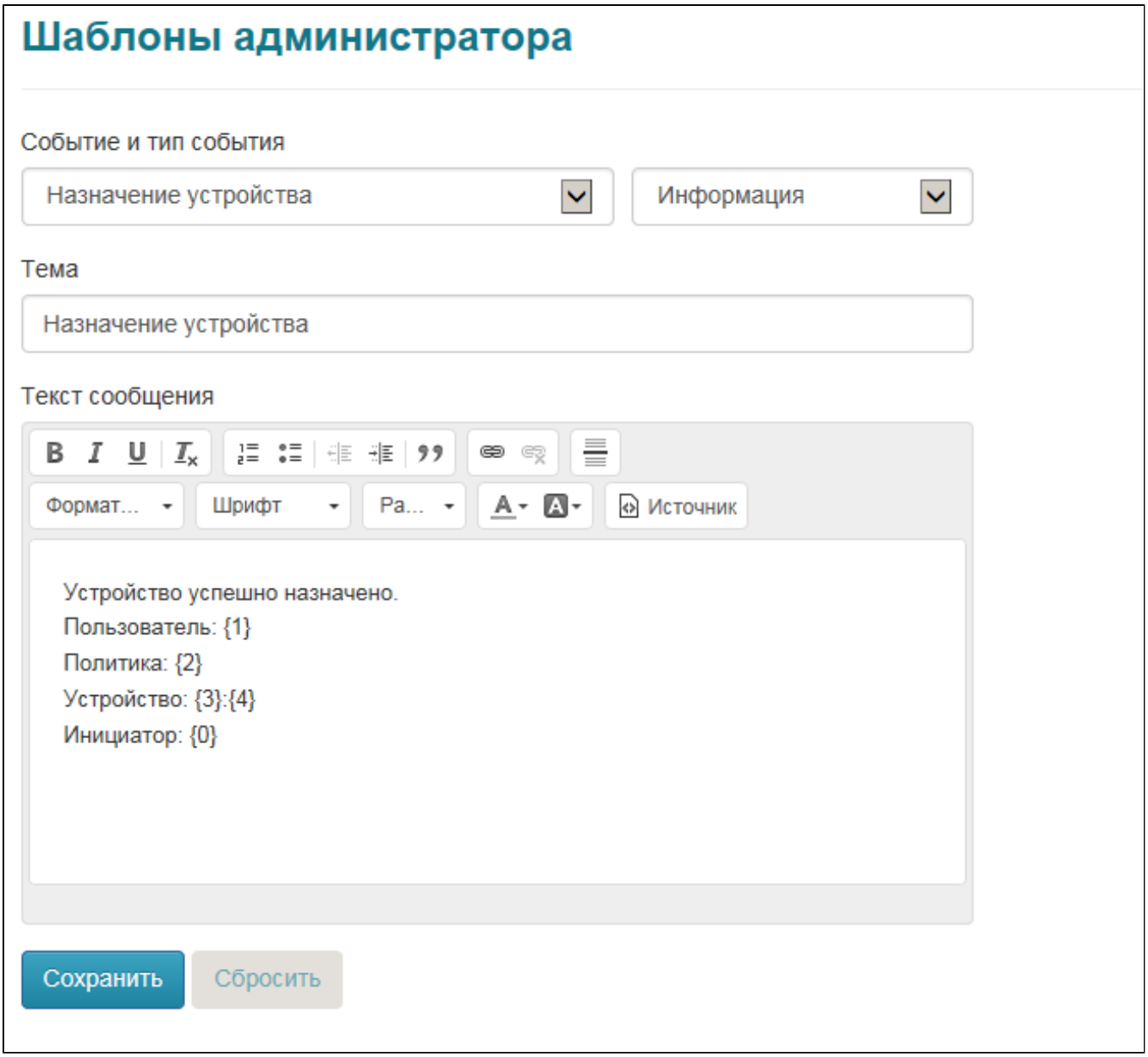
2. Выберите событие, уведомление о котором необходимо отправить, типы события установив соответствующие флаги и нажмите на кнопку **Создать**:



Для редактирования информации об уведомлении нажмите на пиктограмму в строке уведомления, информацию о котором нужно изменить, внесите необходимые изменения и нажмите на кнопку **Сохранить** .

Для удаления уведомления нажмите на пиктограмму в строке уведомления, информацию о котором нужно удалить, и подтвердите удаление.

В разделе **Шаблоны администратора** настраиваются шаблоны почтовых уведомлений о событиях системы, которые будут рассылаться сотрудникам, занимающимся администрированием системы. Для каждого уведомления в рамках одной политики использования смарт-карт можно настроить один шаблон.
В базовом варианте почтовое уведомление содержит следующую информацию:
• **Тема**. Формируется исходя из названия события, например, «Выпуск карты».
• **Текст сообщения**. Формируется исходя из названия сообщения и его типа, может содержать информацию об инициаторе, пользователе и устройствах.



Вместо тэгов в фигурных скобках в письмо будет подставлено соответствующее тэгу значение:

Тэг	Значение
{0}	Инициатор - пользователь, который инициировал событие.
{1}	Пользователь - пользователь, с устройством или учетной записью которого произошло событие.
{2}	Политика, которая распространяется на пользователя, с устройством или учетной записью которого произошло событие.
{3}	Модель устройства, с которым было произведено действие.
{4}	ID устройства, с которым было произведено действие.

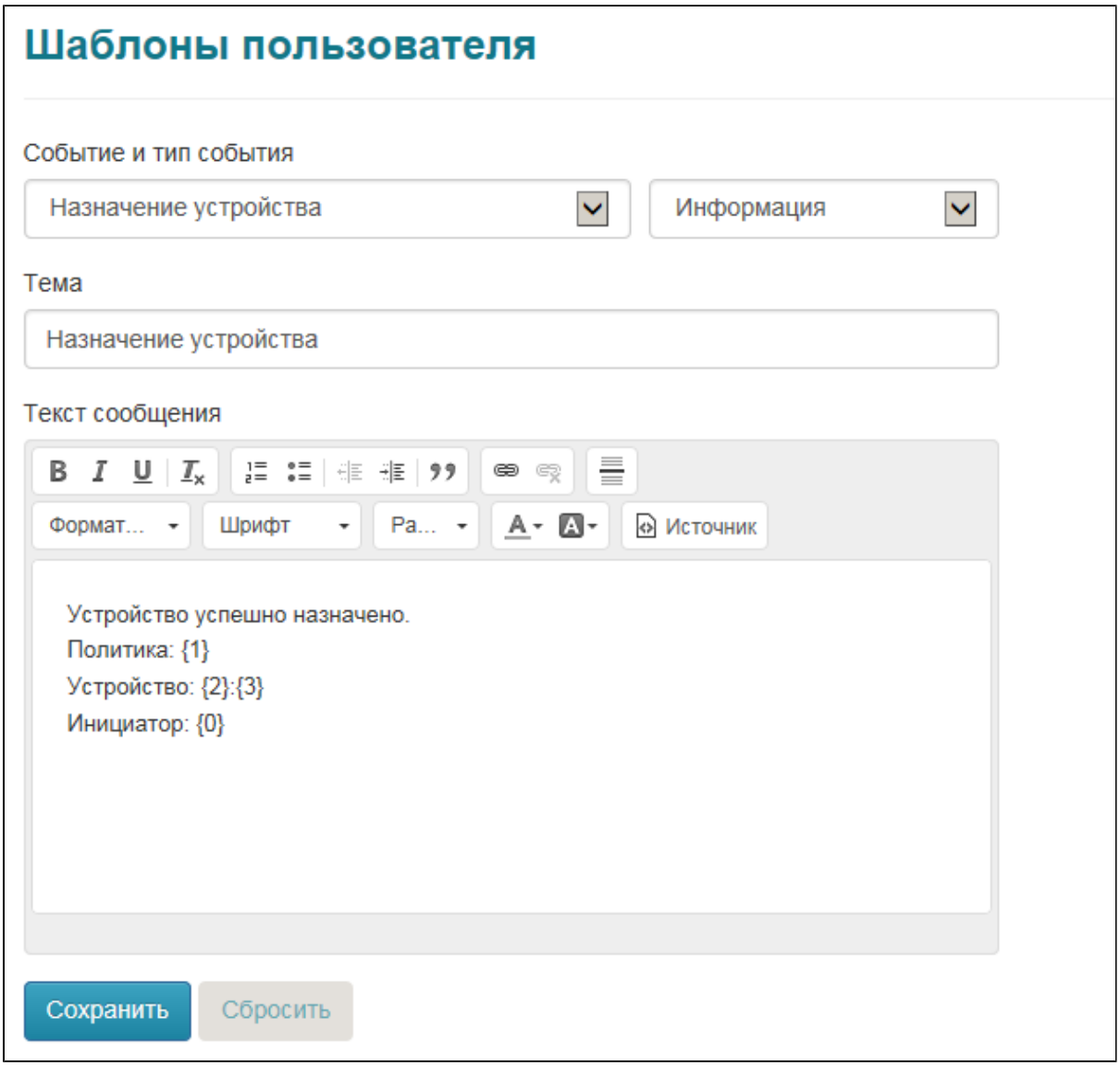
Базовый шаблон может быть изменен в зависимости политики безопасности, используемой в вашей компании. Например, текст письма может быть дополнен сообщением о конфиденциальности содержащейся в нем информации, либо дополнен указаниями к действиям, которые должны предпринять сотрудники, получившее данное письмо.

После внесения изменений в шаблон необходимо нажать на кнопку **Сохранить.**

Шаблон будет сохранен. Сообщения, отправляемые системой при наступлении события, для которого был создан новый шаблон, будут соответствовать созданному шаблону.

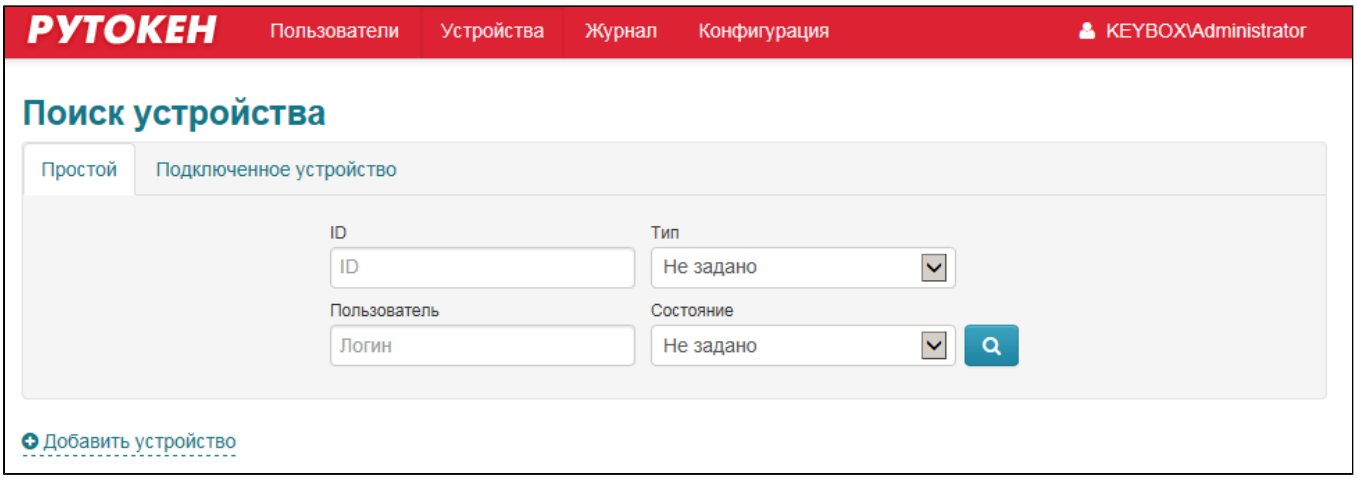
Группа настроек **Шаблоны пользователя** позволяет настроить шаблоны почтовых уведомлений о событиях системы, которые будут рассылаться пользователям системы. Для каждого уведомления в рамках одной политики использования сустройств можно настроить один шаблон.

Шаблоны пользователя настраиваются аналогично шаблонам администратора.



Устройства

Раздел **Устройства** предназначен для получения информации об устройствах, зарегистрированных в системе, а также их регистрации.



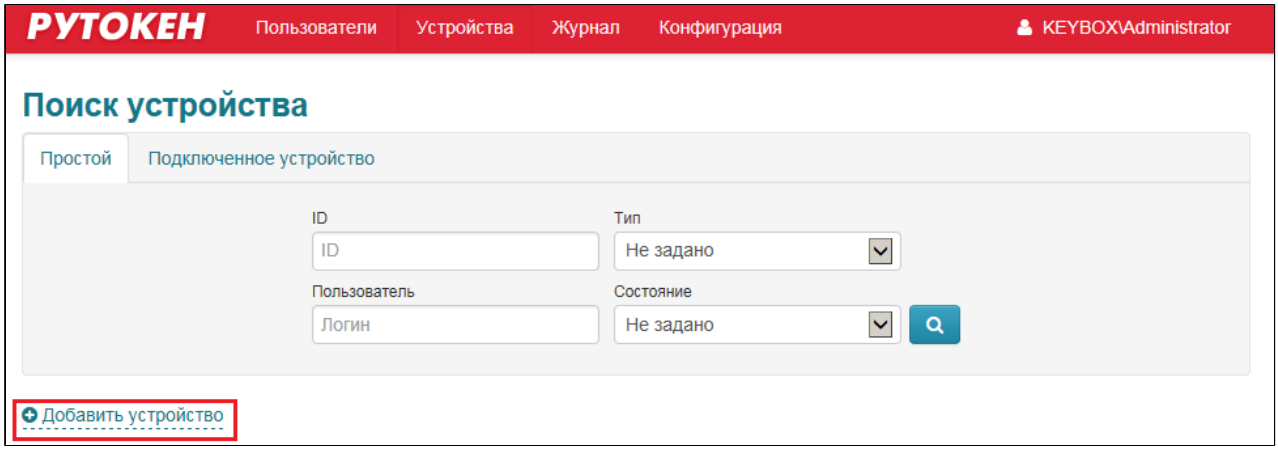
Работа с устройством в системе возможна после его добавления.

Добавление устройства

В процессе добавления в системе сохраняется информация об устройстве. Новый PIN-код Администратора генерируется и сохраняется в системе в зашифрованном виде. В дальнейшем он используется для проведения операций разблокировки и сброса PIN-кода пользователя.

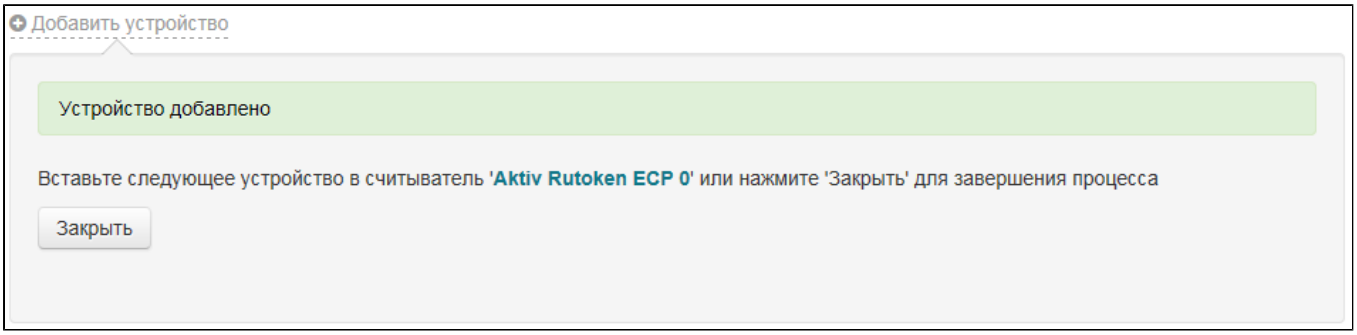
Для добавления устройства в систему:

1. Откройте раздел устройства и нажмите на ссылку **Добавить устройство**:



2. Подключите устройство, выберите в выпадающем списке соответствующий считыватель (если подключено только одно устройство, то считыватель будет определен автоматически) и нажмите на кнопку **Добавить**:

Устройство будет добавлено. Если необходимо добавить еще одно устройство, то подсоедините его к компьютеру. Если все необходимые устройства добавлены, то нажмите на кнопку **Закрыть**.



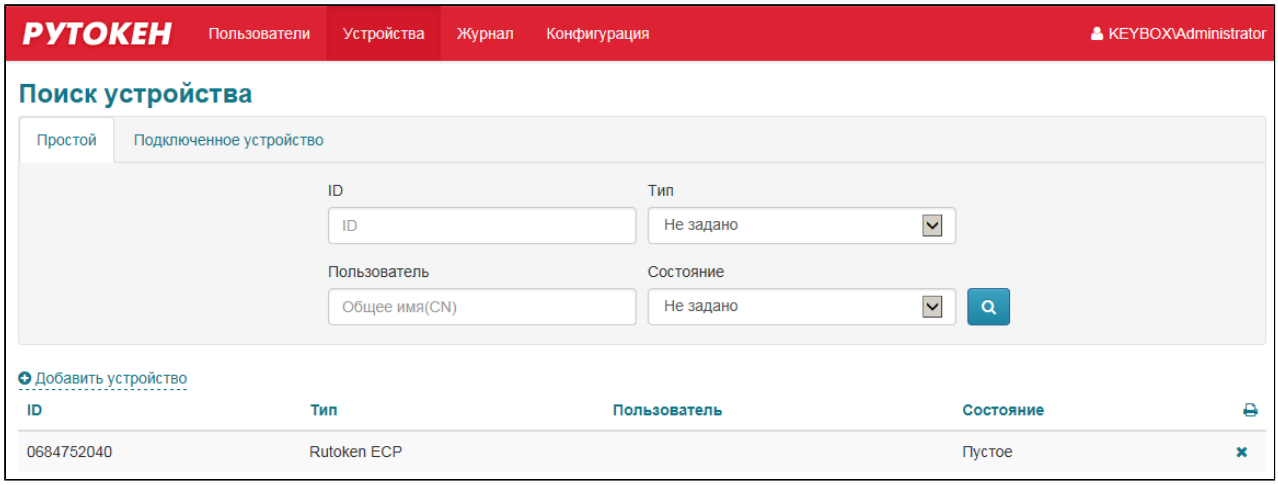
После добавления устройство может быть назначено пользователю и выпущено.

Поиск устройства

Рутокен KeyBox позволяет производить поиск информации об устройстве двумя способами:

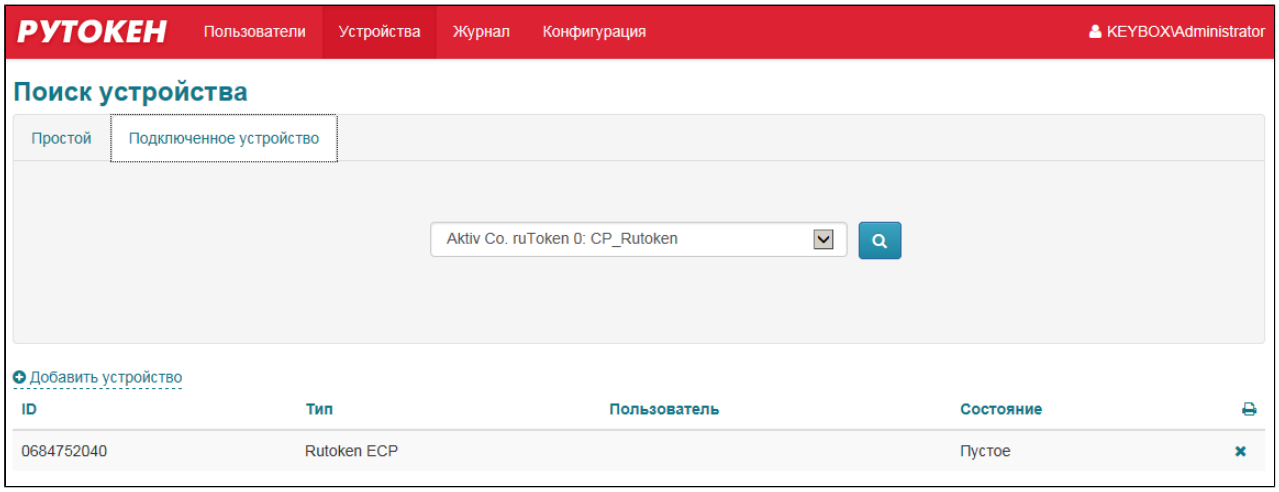
1. Поиск информации об устройстве по параметрам. Применяется в случае, когда физически устройство недоступно, но есть информация о нем (ID устройства, Тип, логин пользователя, которому устройство было назначено, состояние устройства) или если необходимо получить информацию о нескольких устройствах, объединенных общим признаком.

   Для поиска устройства по параметрам заполните необходимые поля и нажмите на кнопку  :



   Если необходимо вывести полный список устройств, введите * в поле ID и нажмите на кнопку  .

2. Поиск информации о подключенном устройстве. Применяется в случае, когда устройство физически доступно.
   Для поиска информации о подключенном устройстве подсоедините его к компьютеру, выберите в выпадающем списке соответствующий считыватель (если подключено только одно устройство, то считыватель будет определен автоматически) и нажмите на кнопку  :



Если устройство было назначено пользователю, то от результатов поиска можно перейти в карточку пользователя для выполнения операций с устройством.

Если устройство назначено пользователю, то можно перейти от результатов поиска к его карточке. Для этого необходимо нажать на ссылку с именем пользователя в столбце **Пользователь**.

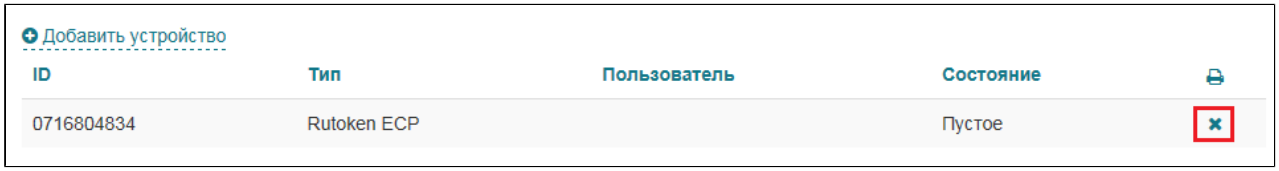
Удаление устройства

В случае, если устройство не было назначено пользователю или было изъято у него, информацию об устройстве можно удалить из системы. Удалить устройство, назначенное пользователю невозможно.

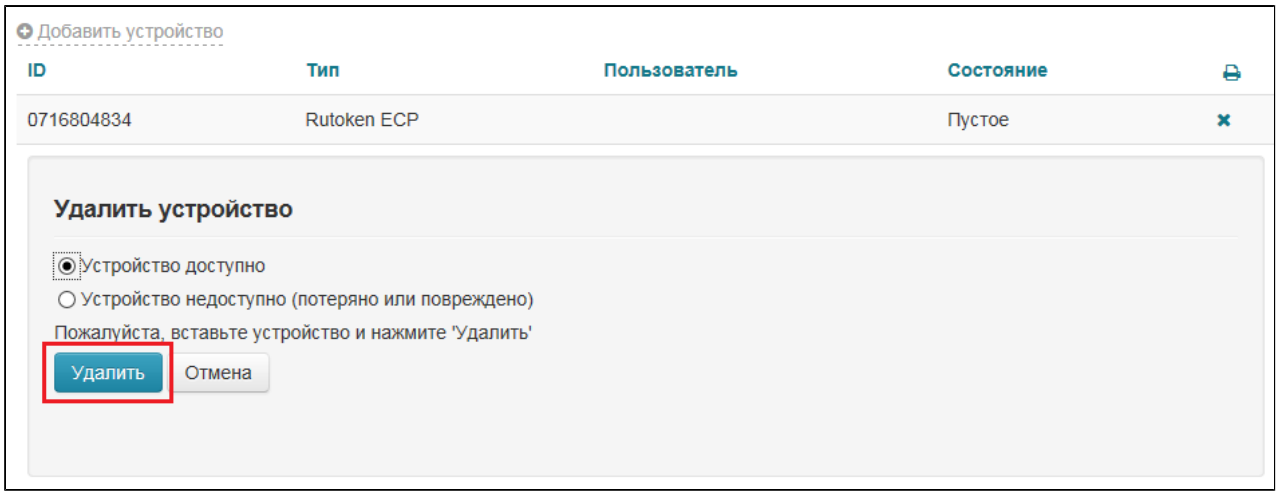
Удаление информации об устройстве из системы возможно как при его наличии, так и без него.

Для удаления информации об устройстве:

1. Выполните поиск информации об устройстве.
2. Нажмите на пиктограмму  в строке устройства, информацию о котором необходимо удалить:



3. В зависимости от того, доступно устройство или нет, выберите соответствующий пункт и нажмите на кнопку **Удалить**. В случае если устройство доступно в процессе удаления из его памяти будут стерты ключевые контейнеры и сертификаты, выпущенные системой:



Информация об устройстве удалена из системы.

Пользователи

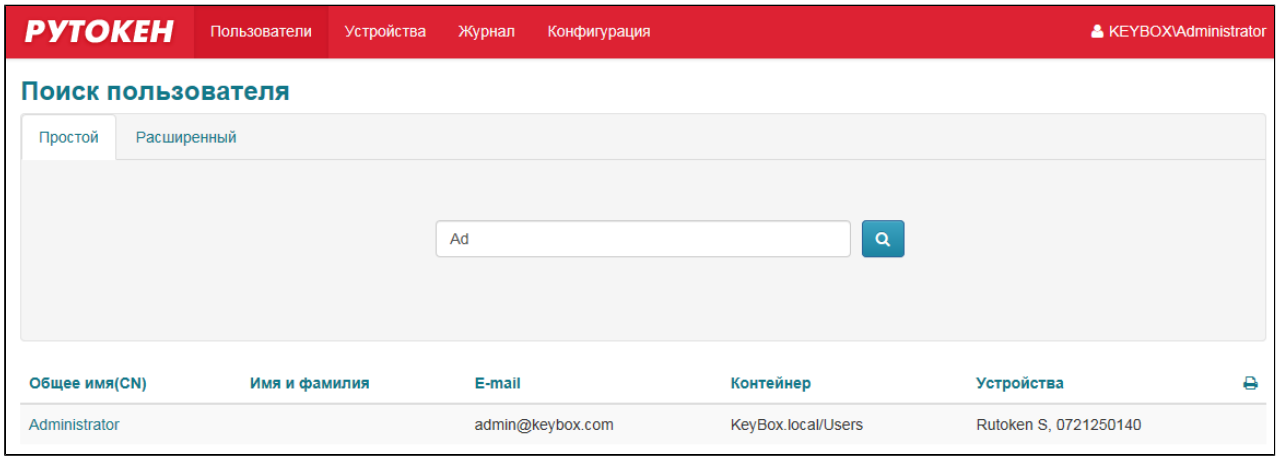
Раздел предназначен для получения информации о пользователях и назначенных им устройствах, проведения операций с устройствами.

Информация о пользователях берется из контейнеров Active Directory.

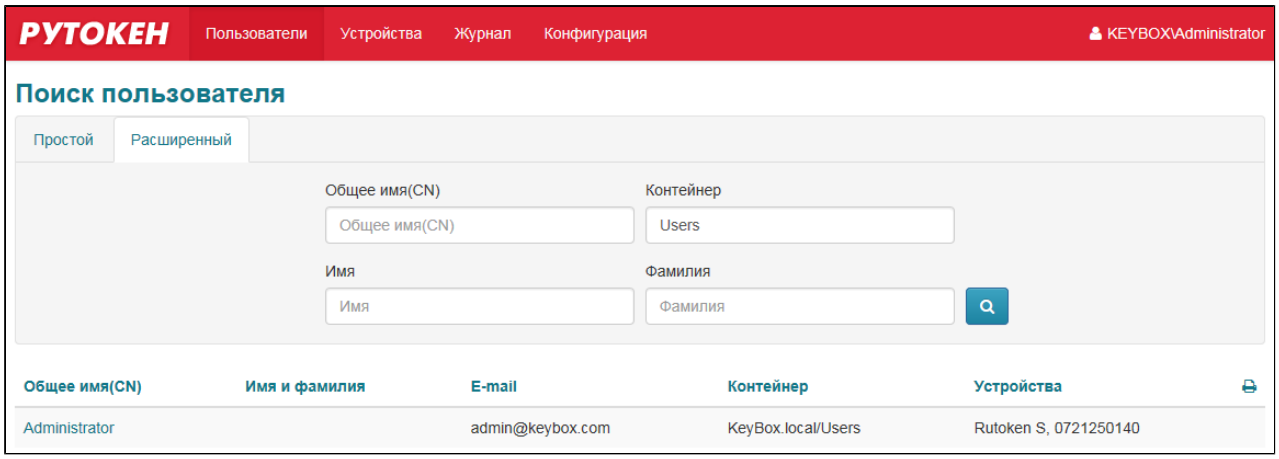
В системе реализовано два типа поиска пользователей:

1. Простой поиск. Позволяет произвести быстрый поиск по одному из параметров (логин пользователя, e-mail, имя или фамилия). Возможен поиск по подстроке.

   Для осуществления поиска введите необходимый параметр в поле и нажмите на кнопку  :



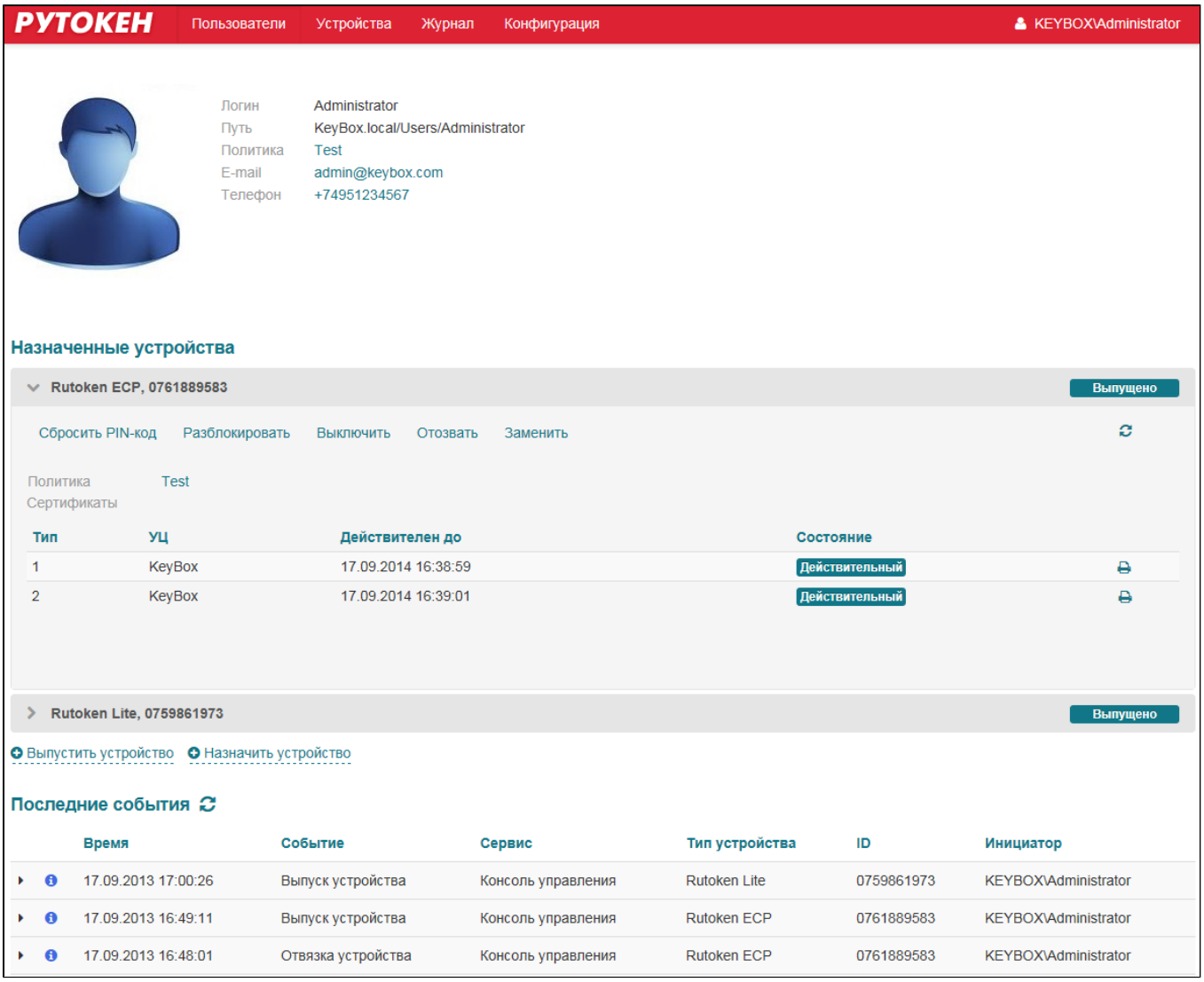
2. Расширенный поиск. Позволяет искать пользователей по нескольким параметрам (логин, контейнер Active Directory, в котором хранится учетная запись пользователя, имя, фамилия). Если какой-то параметр не указан, то он не учитывается при поиске.
   Для осуществления поиска по нескольким параметрам введите необходимые данные и нажмите на кнопку  :



В результатах поиска будет отображена следующая информация о нем:

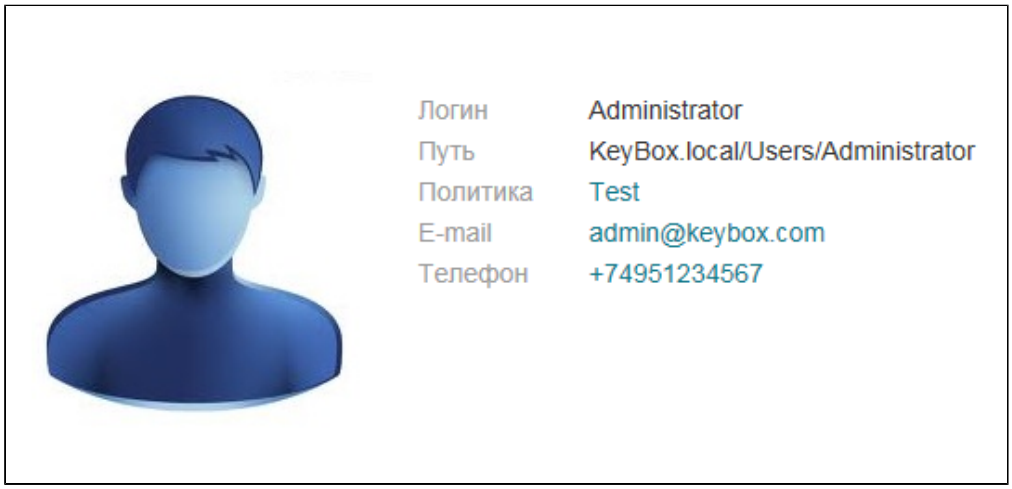
Поле	Значение
Логин	логин пользователя в домене.
Имя и фамилия	имя и фамилия пользователя.
E-mail	e-mail пользователя.
Контейнер	полный путь к контейнеру Active Directory, в котором хранится учетная запись пользователя.

Для каждого пользователя системы формируется карточка пользователя, в которой можно просмотреть информацию о назначенных ему устройствах и произвести ряд операций с ними. Переход в карточку пользователя осуществляется из результатов поиска:

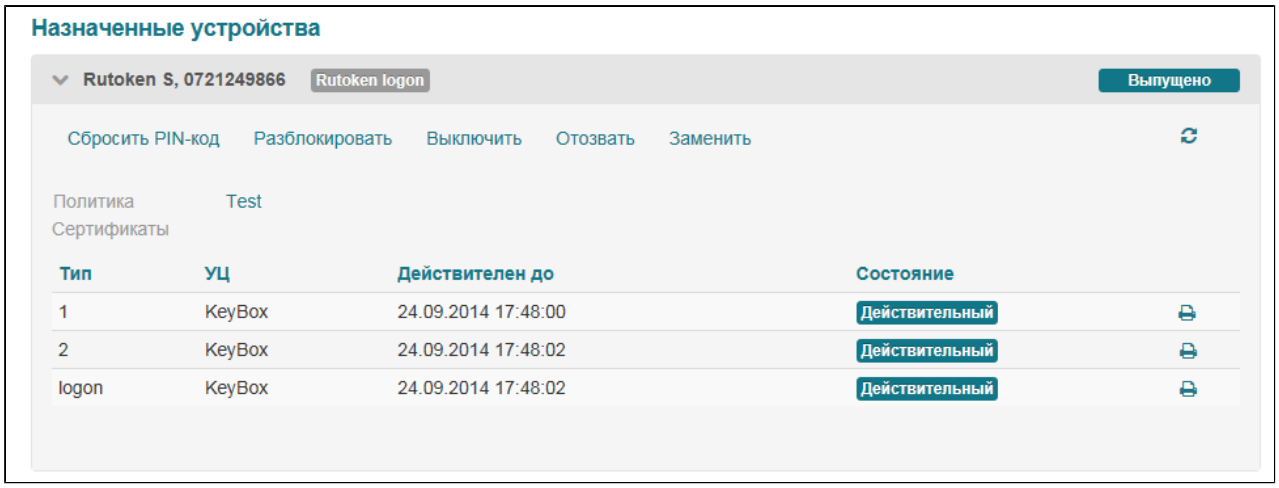


В карточке пользователя отображена следующая информация:

1. Информация о пользователе:



2. Информация об устройствах, назначенных пользователю (тип устройства, ID, состояние, политика, при которой оно выпускалось, информация о выпущенных сертификатах):



Возможные состояния устройства:

Состояние	Описание
Назначено	Устройство привязано к учетной записи пользователя, но еще не выпущено
Выпущено	Устройство привязано к учетной записи пользователя и выпущено
Выключено	Устройство временно выключено
Отозвано	Устройство отозвано в связи с поломкой, утерей или обновлением
В ожидании	Запрос на сертификат ожидает рассмотрения администратором

Возможные состояния сертификатов:

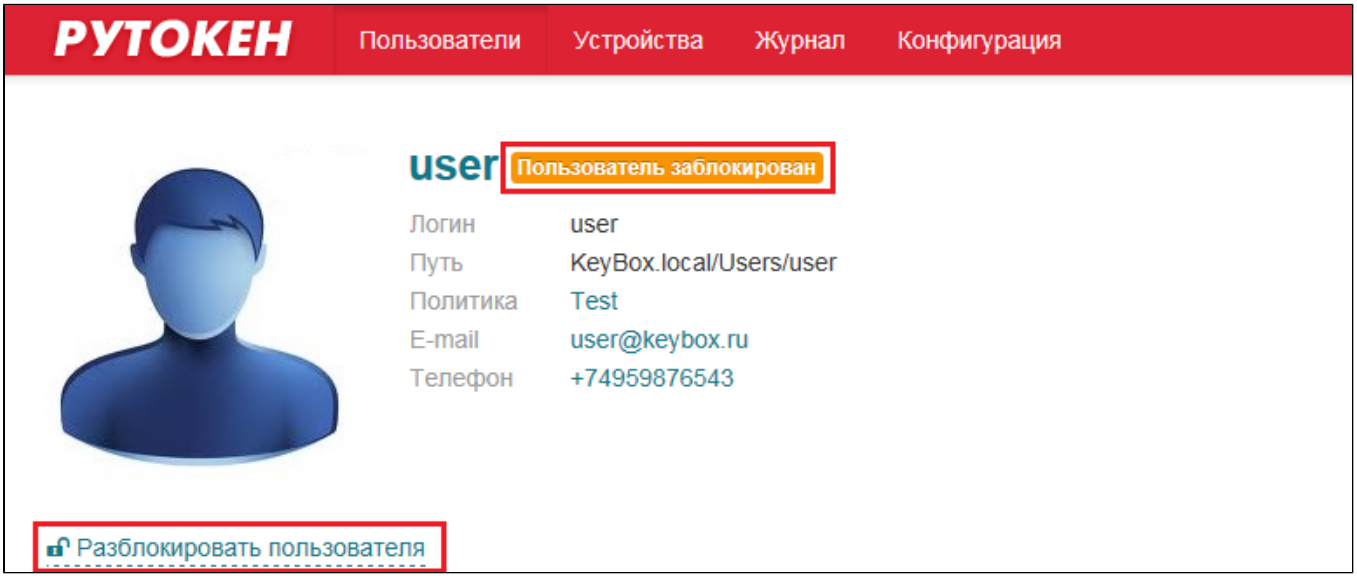
Состояние	Описание
Действительный	Сертификат действителен
Истекает	Срок действия сертификата скоро закончится
Истек	Срок действия сертификата истек, требуется обновить сертификат
Отозван	Сертификат отозван
В ожидании	Запрос на сертификат ожидает рассмотрения администратором
Одобрен	Запрос на сертификат одобрен администратором, но сертификат еще не выпущен пользователю
Отклонен	Запрос на сертификат отклонён администратором
Ошибка	Состояние сертификата не удалось определить. Возможно, центр сертификации недоступен. Сертификат не пригоден для использования

3. Информация о последних действиях с учетной записью пользователя и его устройствами в системе (время, событие, источник события, тип устройства, ID устройства (если событие связано с устройством), инициатор события):

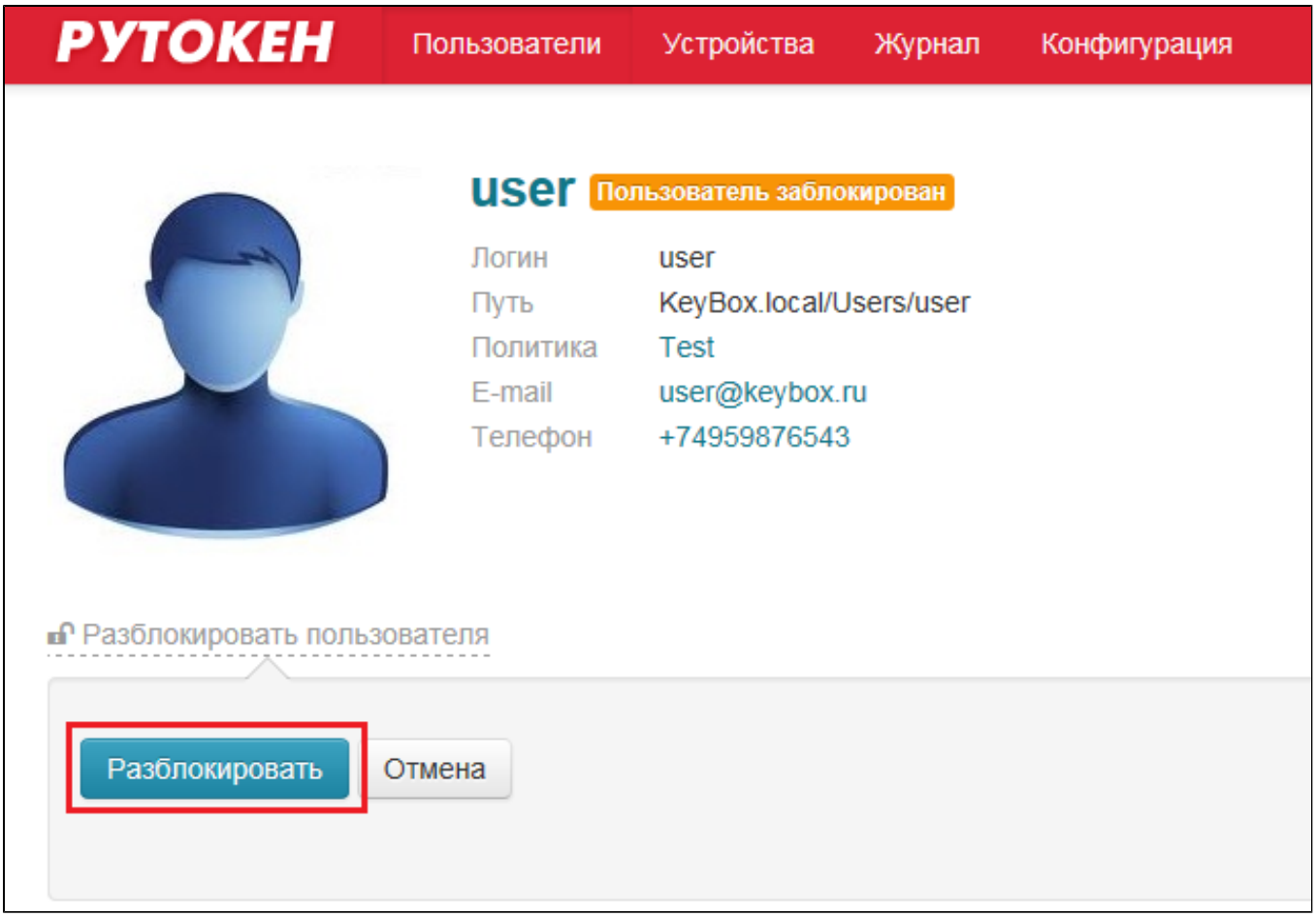
Разблокировка учетной записи

В случае если пользователь вводит неверные ответы на секретные вопросы установленное в политике число раз, его учетная запись в системе блокируется. При блокировке пользователь не может получить доступ в удаленный личный кабинет, а так же к другим операциям системы, требующим аутентификации по секретным вопросам. На учетную запись MS Windows и сертификаты пользователя блокировка не влияет.

В карточке заблокированного пользователя появляется соответствующая отметка и ссылка **Разблокировать пользователя**:



Для разблокировки пользователя нажмите на ссылку **Разблокировать пользователя** и подтвердите разблокировку нажатием на кнопку **Разблокировать**:

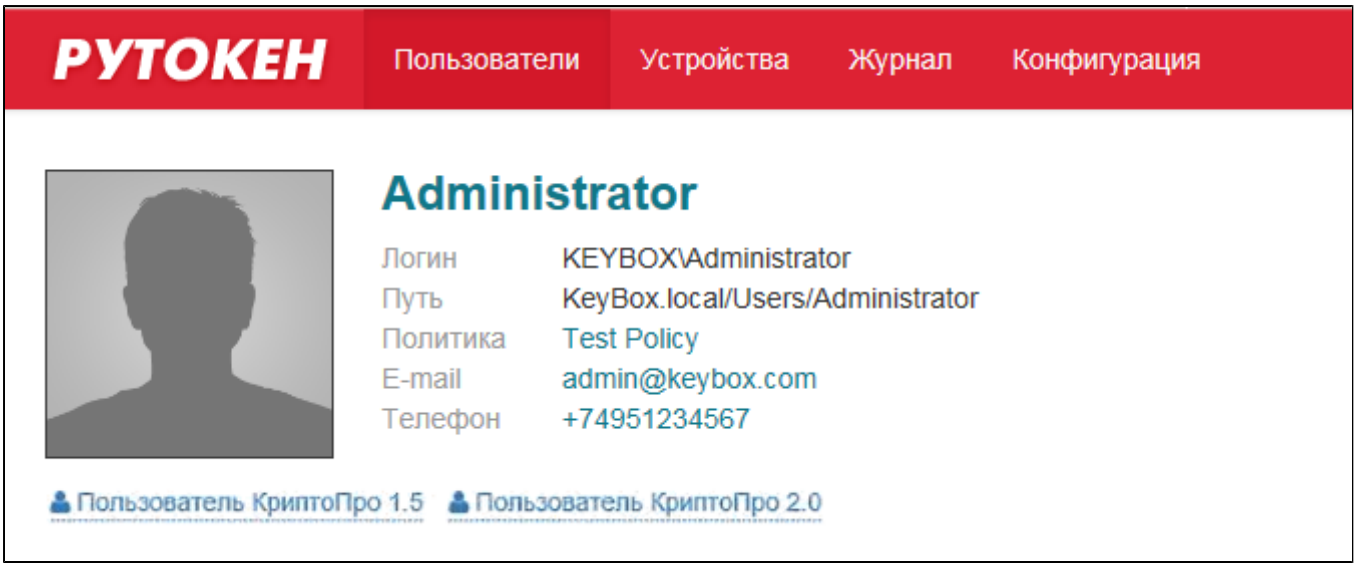


После этого учетная запись пользователя будет разблокирована. Доступ к удаленному личному кабинету восстановлен.

Связь пользователя Рутокен KeyBox с каталогом УЦ

Если в используемой вами конфигурации каталог пользователей Рутокен KeyBox не совпадает с каталогом пользователей удостоверяющего центра (например, пользователям Active Directory необходимо выпускать сертификаты УЦ КриптоПро 1.5 и 2.0), то для выпуска смарт-карты необходимо установить связь с каталогом нужного удостоверяющего центра.

Необходимость привязки пользователя к каталогу удостоверяющего центра определяется в политике использования смарт -карт (раздел **Удостоверяющие центры**, опция **Устанавливать привязку между пользователем УЦ и пользователем каталога**). Один и тот же пользователь Active Directory может быть связан с каталогами различных УЦ. В карточке пользователя, на которого распространяется политика с двумя удостоверяющими центрами КриптоПро, есть возможность связи с каталогами этих УЦ:



Пользователь Рутокен KeyBox (не важно, в каком каталоге он расположен: Active Directory, КриптоПро 1.5 или 2.0) может быть связан с любым пользователем удостоверяющих центров КриптоПро 1.5 и 2.0. Если каталог УЦ, с которым необходимо установить связь, не содержит пользователей, то при помощи Рутокен KeyBox их можно создать.

Связь пользователя Active Directory с пользователем КриптоПро УЦ 1.5

1. Перейдите в карточку пользователя.
2. Нажмите **Пользователь КриптоПро1.5**.
3. Введите имя пользователя центра регистрации КриптоПро УЦ 1.5 и нажмите кнопку.
4. Отметьте нужного пользователя в результатах поиска и нажмите кнопку *Установить привязку*.
5. Установленную привязку можно отменить. Для этого нажмите **Пользователь КриптоПро1.5** и затем *Отменить привязку*.
6. Если каталог КриптоПро УЦ 1.5 не содержит пользователей, то для установки связи с пользователем Рутокен KeyBox потребуется создать и пользователя удостоверяющего центра. Для этого перейдите на вкладку *Создать*. В случае необходимости можно отредактировать данные создаваемого пользователя. Перечень полей, данные которых доступны для редактирования зависит от настроек используемого удостоверяющего центра КриптоПро.

Важная информация

При создании пользователя КриптоПро УЦ 1.5 некоторые поля свойств могут быть заполнены автоматически. Например, имя пользователя, адрес электронной почты, город, страна. Эти данные Рутокен KeyBox получает из профиля пользователя Active Directory.

Связь пользователя Active Directory с пользователем КриптоПро УЦ 2.0

Связь пользователя с каталогом КриптоПро УЦ 2.0 осуществляется по аналогии с КриптоПро УЦ 1.5. При поиске (и создании) пользователя существует возможность выбора папки (из числа тех, что существуют в центре регистрации) в которой необходимо искать (или разместить в случае создания) пользователя.

Работа с устройством

Специалисты службы технической поддержки системы могут выполнять следующие операции с устройствами в карточке пользователя:

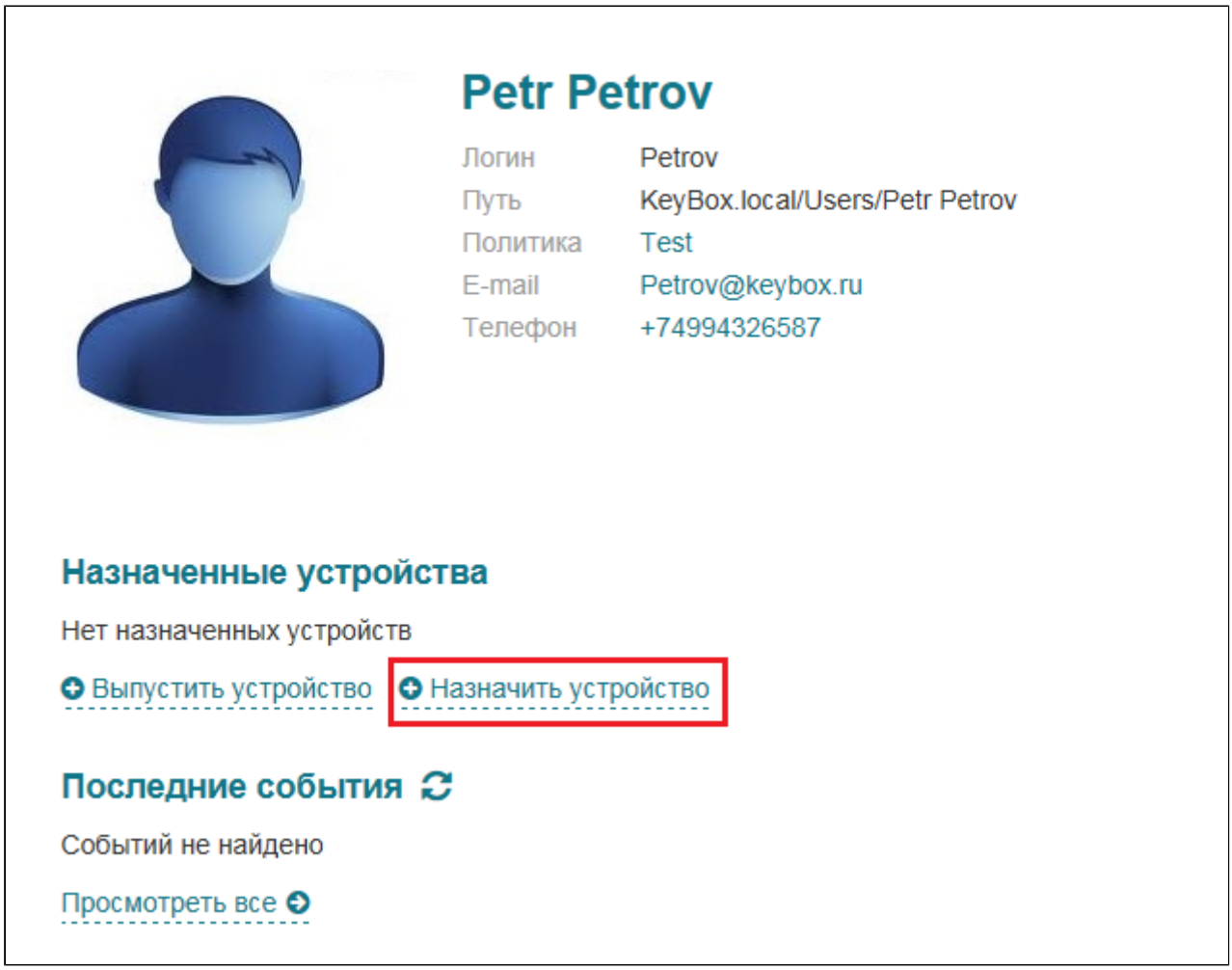
Назначение устройства

В процессе назначения производится привязка устройства, которое уже числится в системе, к учетной записи пользователя. После этого пользователь может самостоятельно сгенерировать ключевую пару и выпустить сертификат используя Self Service, если эти действия разрешены действующей политикой.

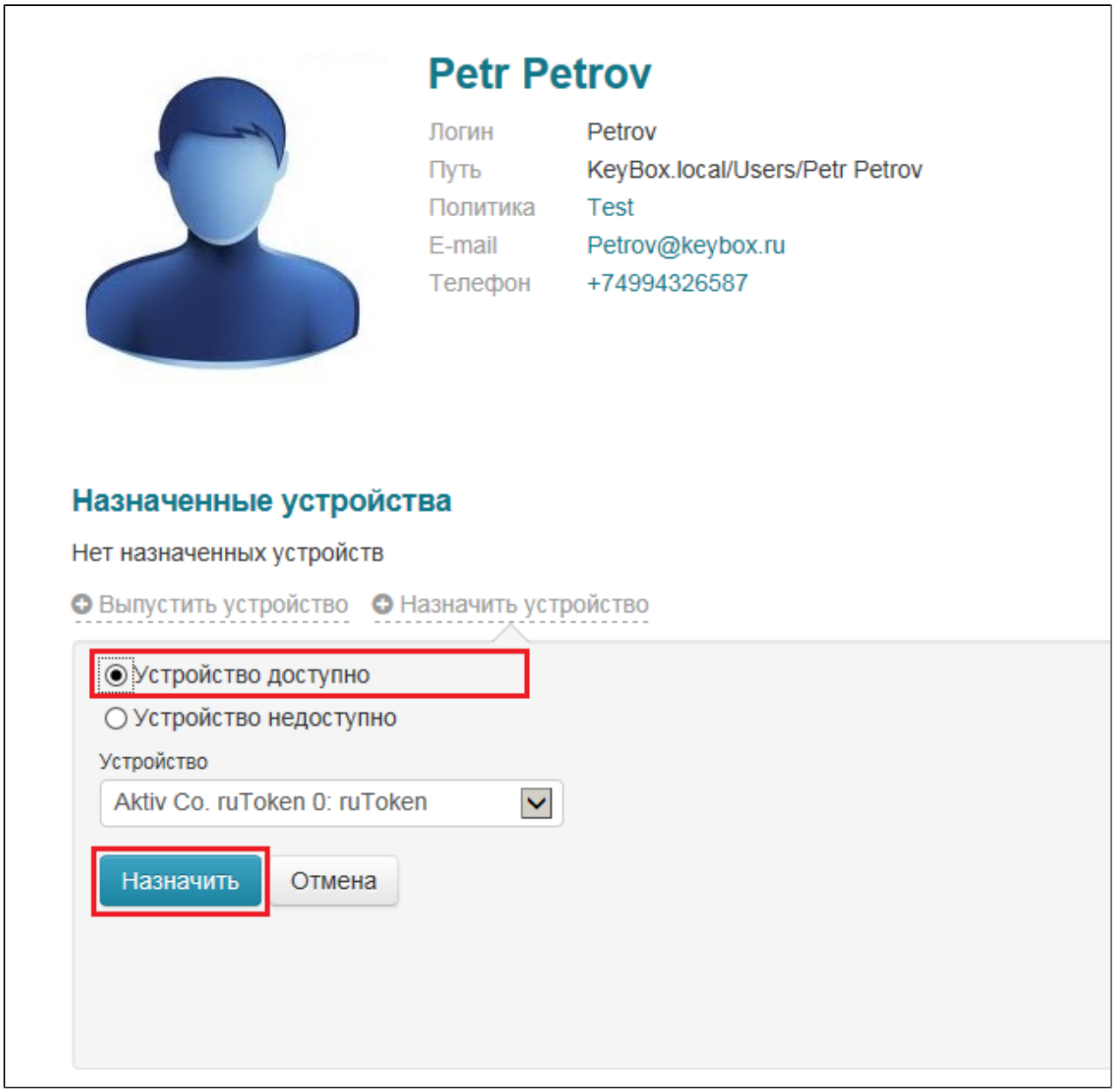
Перед назначением устройства необходимо убедиться в том, что оно числится в системе.

Для назначения устройства пользователю:

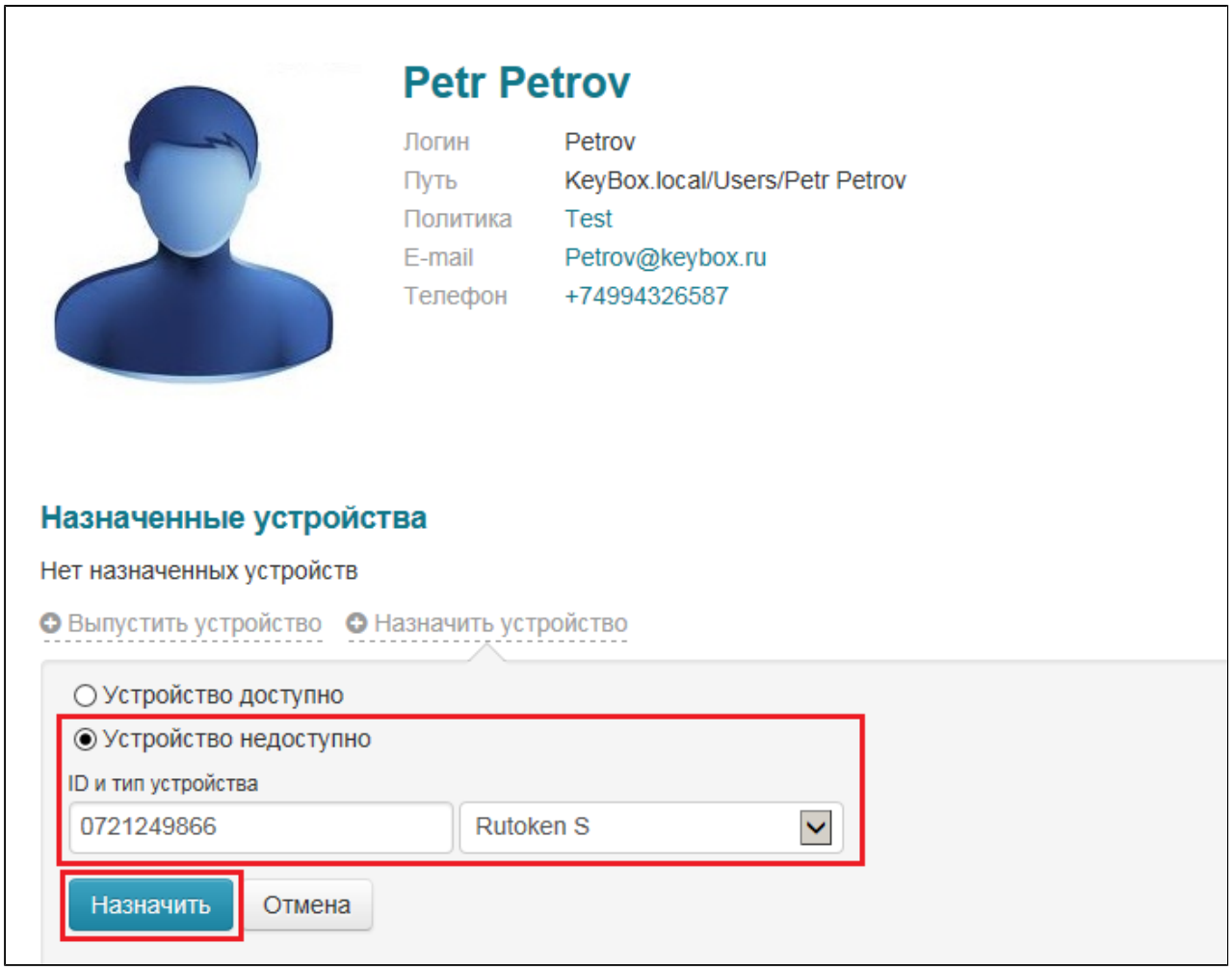
1. Откройте карточку пользователя, которому необходимо назначить устройство и нажмите на ссылку **Назначить устройство**:



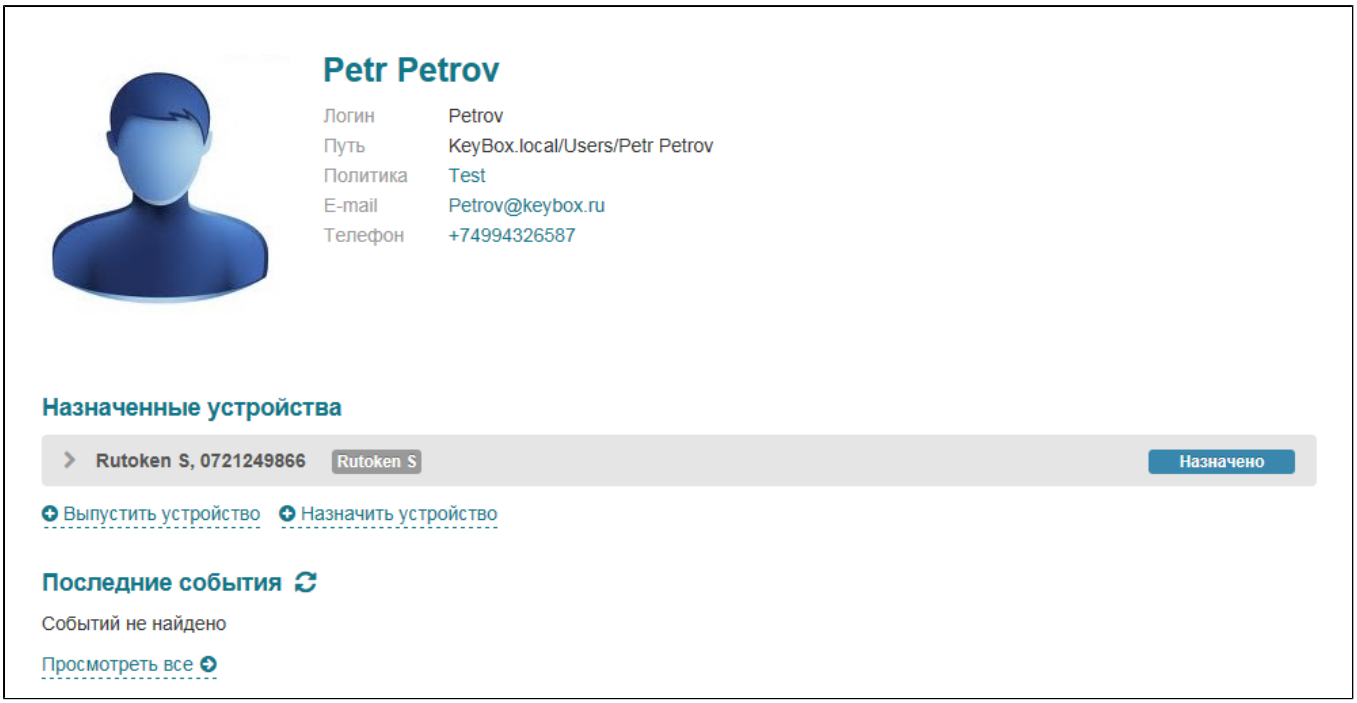
2. Выберите необходимую опцию, если выбрана опция **Устройство доступно**, подключите его и выберите в списке соответствующий считыватель и нажмите на кнопку **Назначить**:



Если устройство недоступно, выберите соответствующий пункт, укажите ID устройства и его тип и нажмите на кнопку **Назначить:**



После этого устройство будет назначено пользователю. Оно появится в списке устройств в карточке пользователя, а также в личном кабинете:



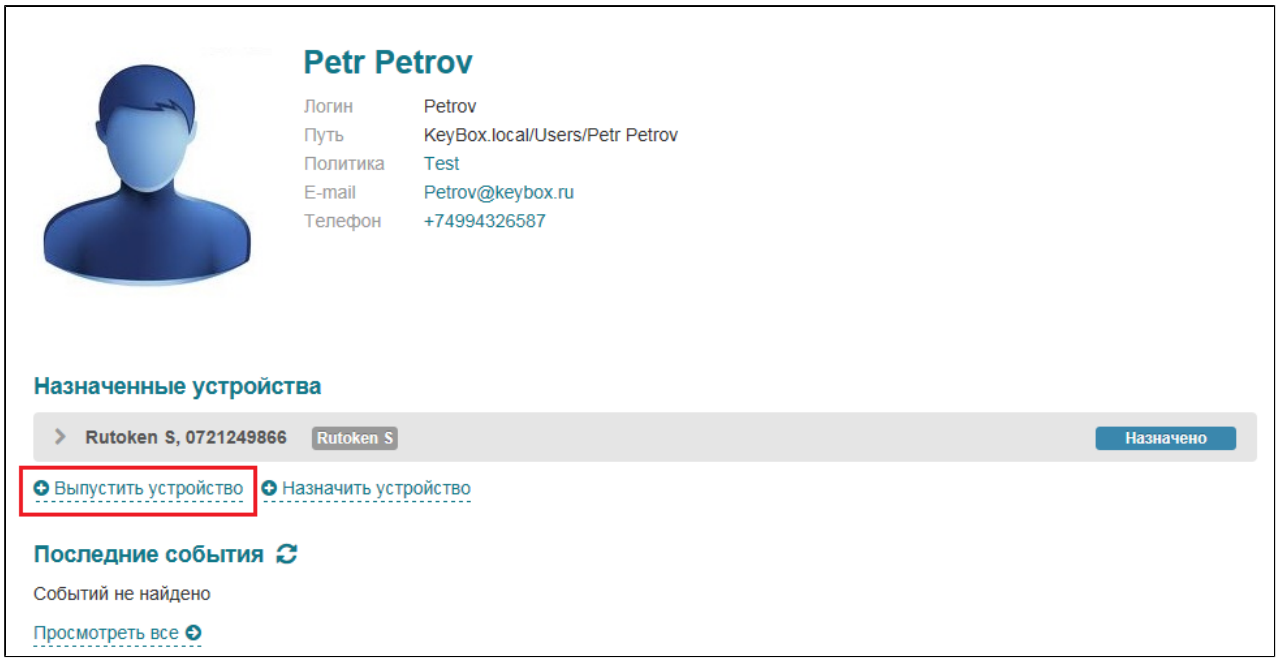
Пользователь может самостоятельно выпустить устройство после его получения, если это разрешено действующей политикой.

Выпуск устройства

Для того чтобы пользователь мог использовать устройство, необходимо провести процедуру выпуска. В процессе выпуска устройство персонализируется: в соответствии с настройками политики производится инициализация, выпускаются сертификаты и происходит их запись в память устройства. Пользователь может выпустить себе устройство самостоятельно, если такая возможность включена в политике.

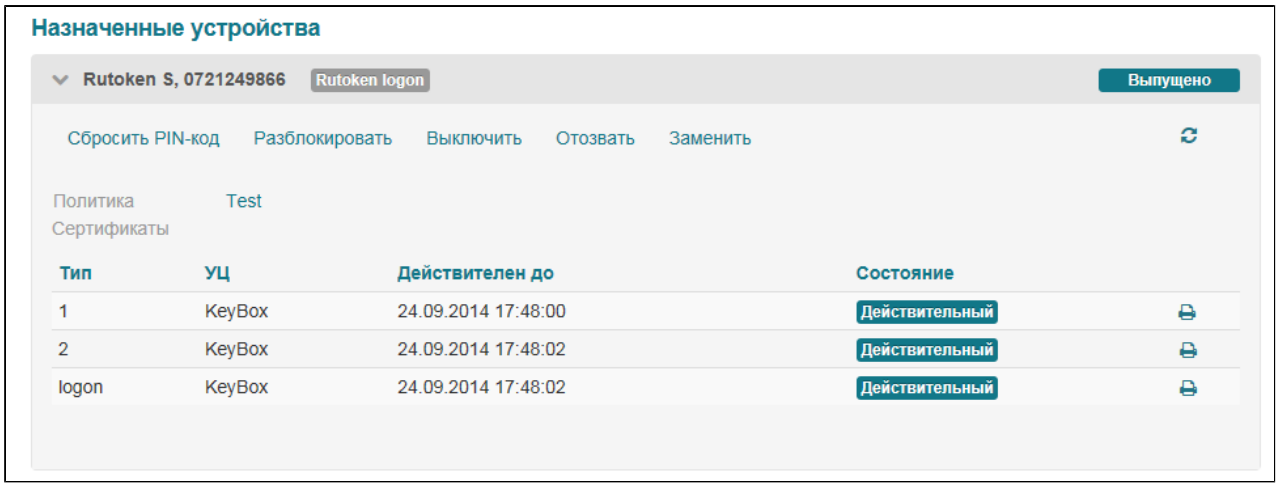
Для выпуска устройства через консоль администратора:

1. Откройте карточку пользователя, которому необходимо назначить устройство и нажмите на ссылку **Выпустить устройство**:



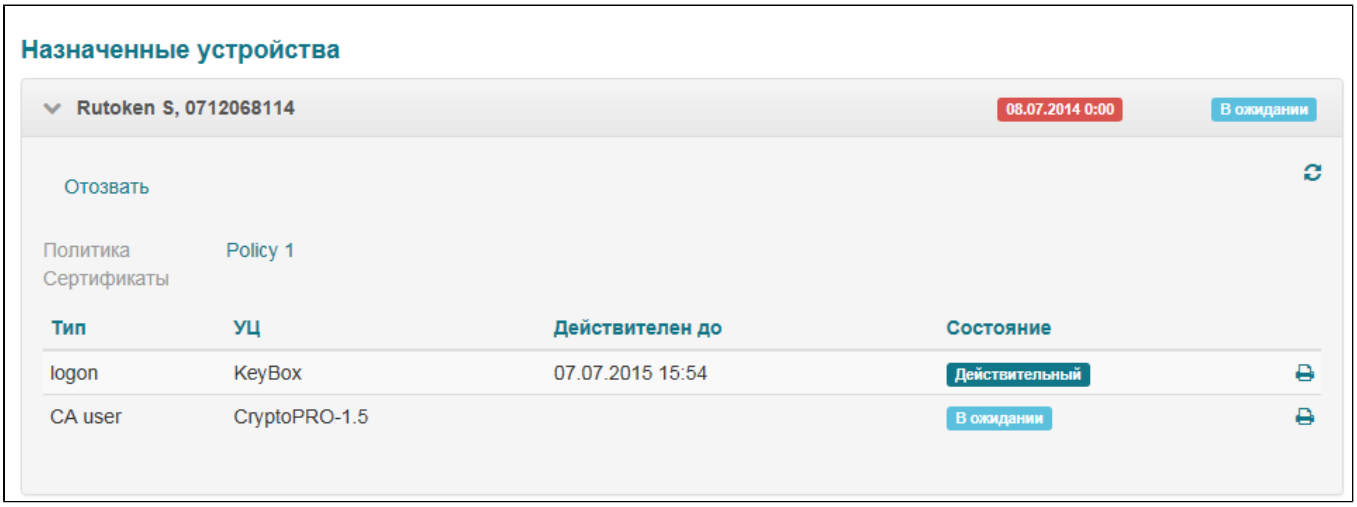
2. Введите имя устройства, если это необходимо, выберите соответствующий считыватель из списка и нажмите на кнопку **Выпустить**:

В процессе выпуска будут выпущены и записаны на устройство сертификаты, предусмотренные политикой для данного пользователя.



В зависимости от настроек политики устройство может быть заблокировано в процессе выпуска. В этом случае пользователю необходимо будет самостоятельно разблокировать устройство при получении.

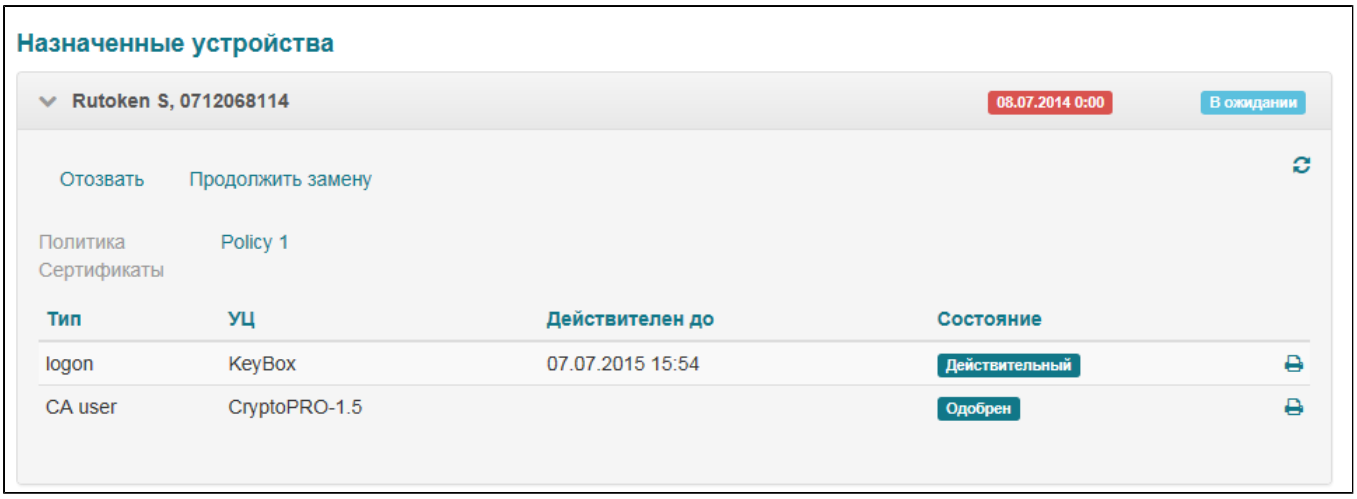
В случае, если один или несколько сертификатов требуют подтверждения, устройство будет находиться в статусе **В ожидании** до тех пор, пока не будет обработан запрос на сертификат. Устройство можно отключить от компьютера, выпуск можно будет завершить после подтверждения запроса.



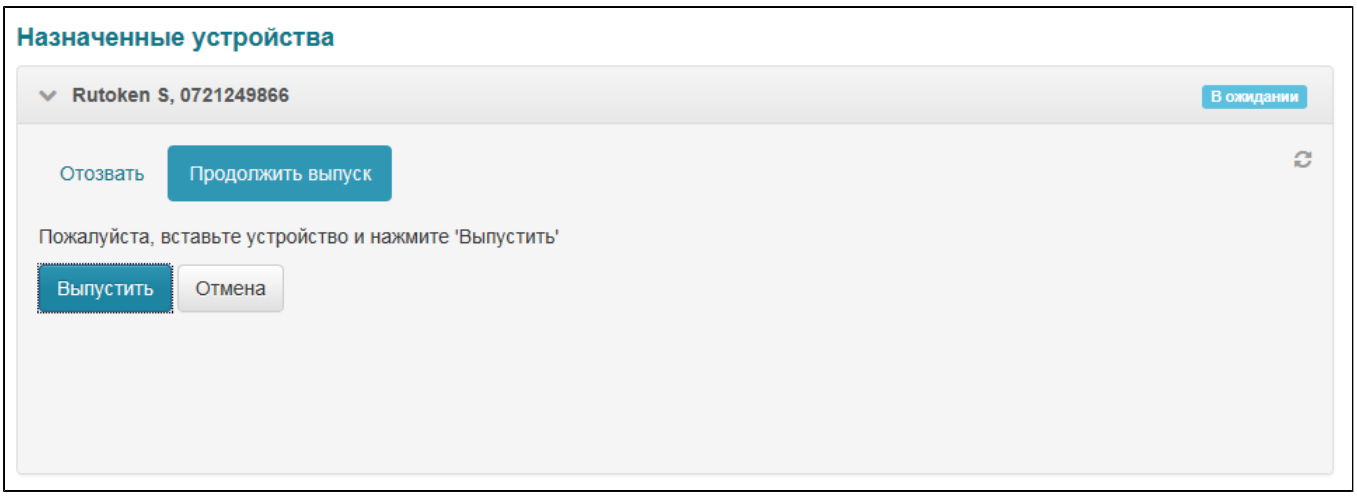
Важная информация

Завершение выпуска устройства невозможно, если хотя бы один из запрашиваемых сертификатов не будет одобрен оператором УЦ.

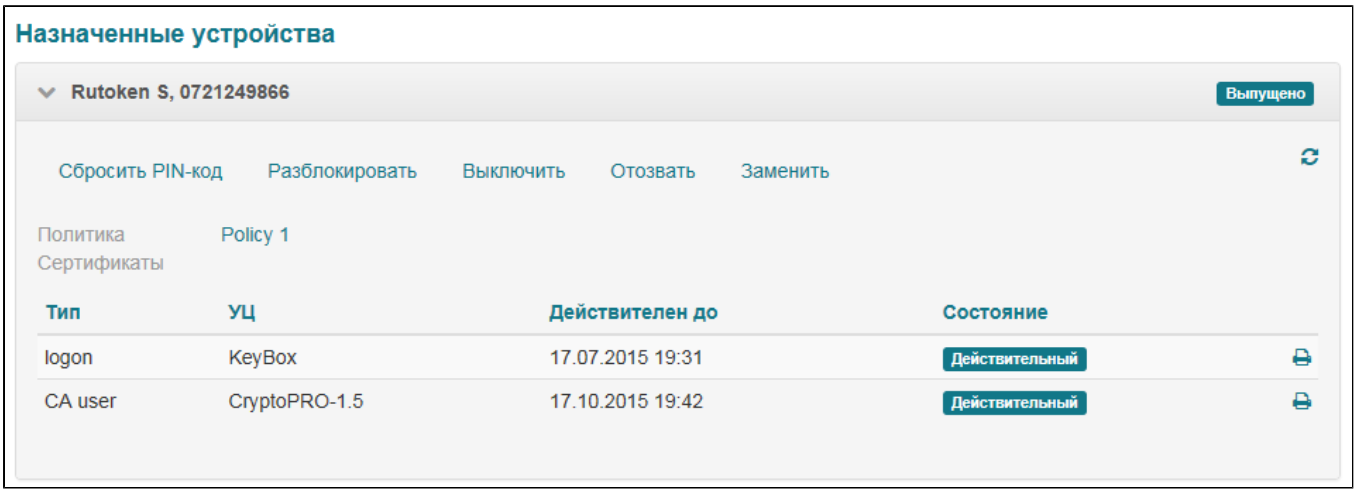
После обработки запроса требуется завершить выпуск. Для этого подключите устройство и нажмите на кнопку **Продолжить выпуск**:



Подтвердите выпуск:



После завершения выпуска все сертификаты будут записаны на устройство. Устройство готово к работе.



Если запрос на сертификат был отклонен, выпуск устройства невозможен.

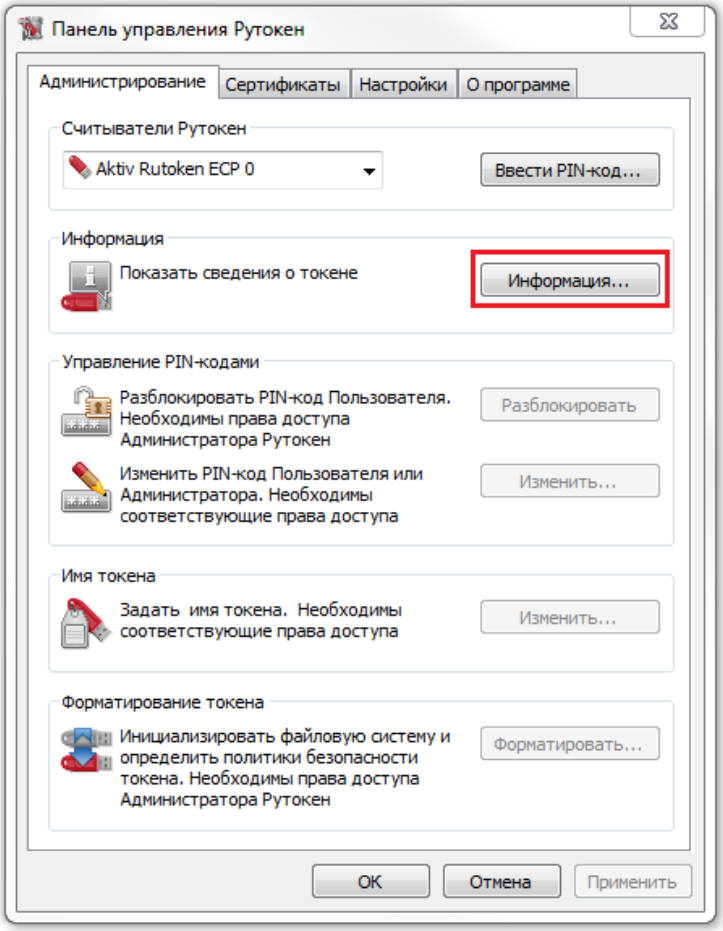
Система позволяет отправлять на печать запросы на сертификат и сами сертификаты. Для того чтобы распечатать запрос или сертификат нажмите на кнопку справа от запроса/сертификата.

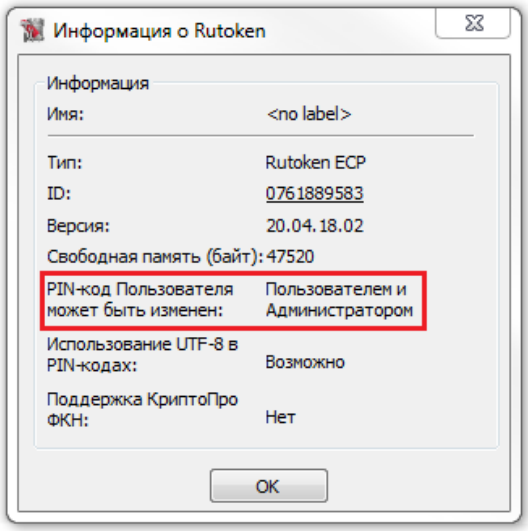
Сброс PIN-кода

В случае если пользователь забыл PIN-код устройства, сотрудник технической поддержки может сбросить его на PIN-код по умолчанию для данного типа устройств. Для сброса PIN-кода необходимо наличие устройства.

Важная информация

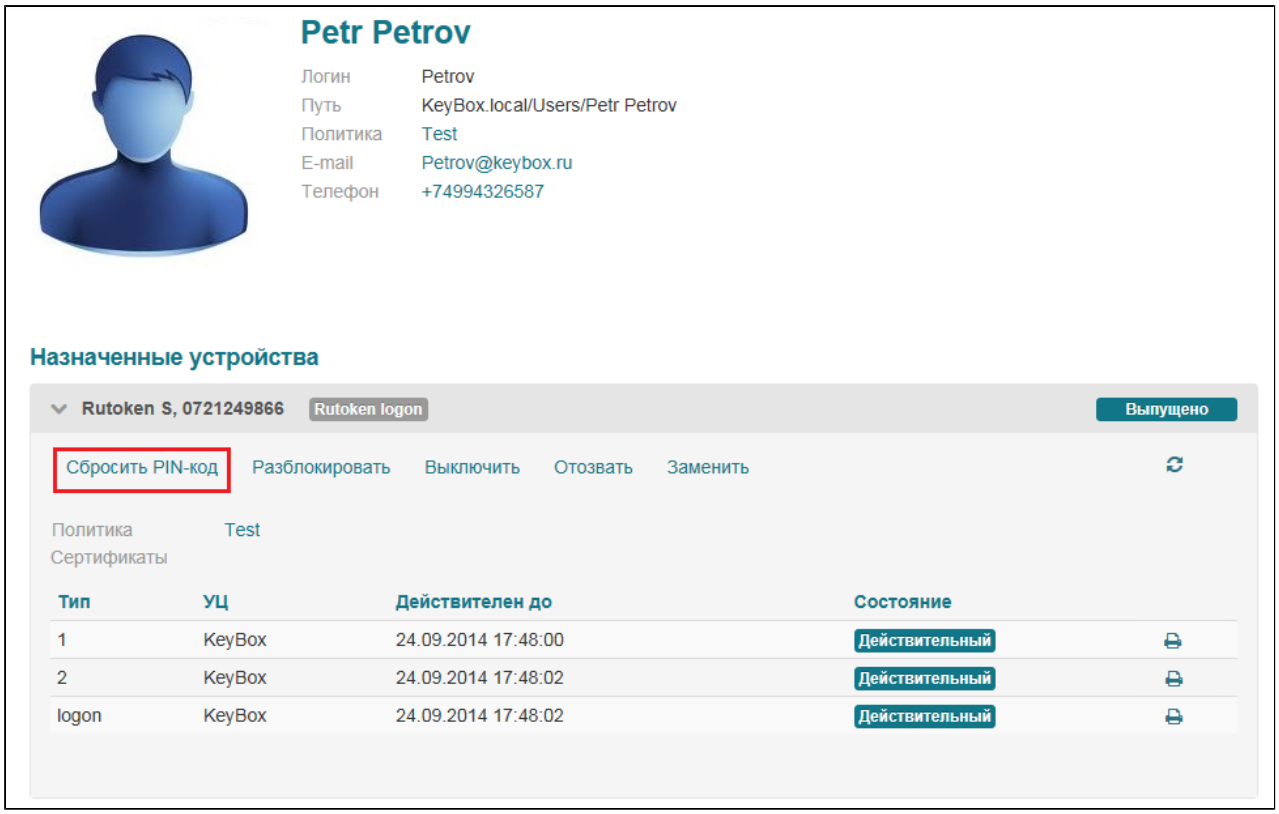
Сброс PIN-кода производится с использованием PIN-кода администратора. Если при форматировании устройства значение параметра **PIN-код Пользователя может быть изменен** установлено в значение **Пользователем**, а не **Пользователем и Администратором**, то сброс PIN-кода будет невозможен. Проверить значение параметра можно запустив **Панель управления Рутокен** (системное меню Пуск\ Программы\ Rutoken\ Панель управления Рутокен) и нажав на кнопку Информация:



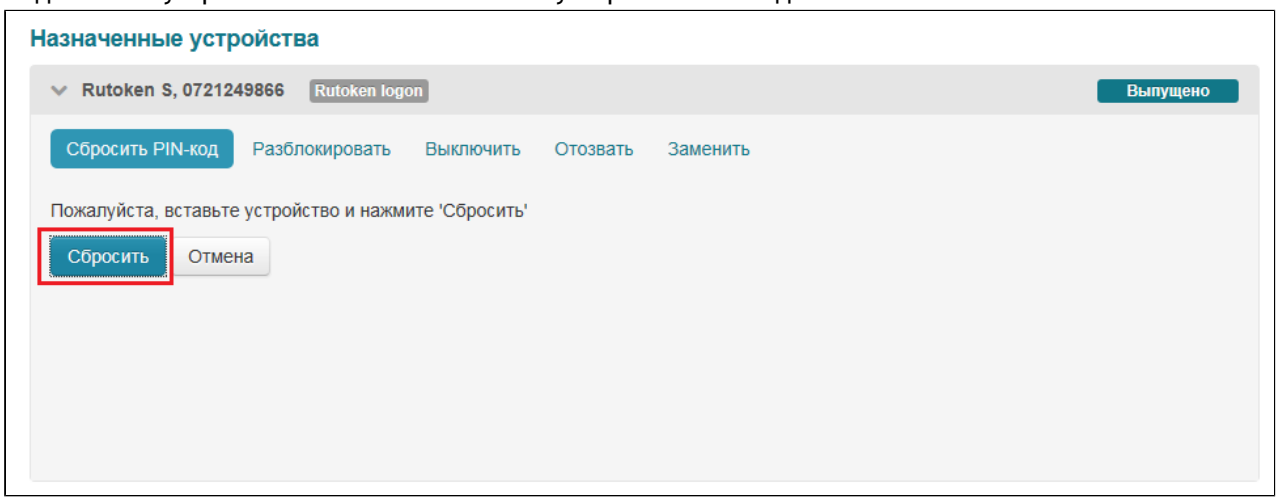


Для сброса PIN-кода:

1. В карточке пользователя в списке назначенных устройств выберите устройство и нажмите на ссылку Сбросить PIN-код:



2. Подключите устройство и нажмите на кнопку Сбросить PIN-код:



PIN-код Пользователя будет сменен на PIN-код по умолчанию.

Разблокировка устройства

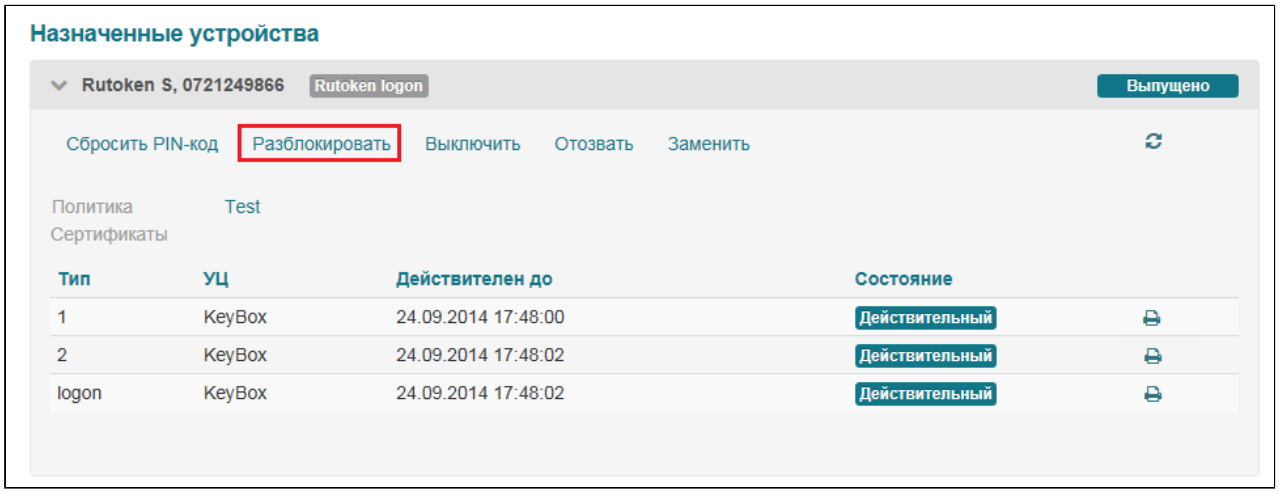
В случае если пользователь вводит неверный PIN-код установленное число раз, устройство блокируется. Для дальнейшей работы с устройством пользователю необходимо разблокировать устройство.

Системой поддерживается несколько способов разблокировки:

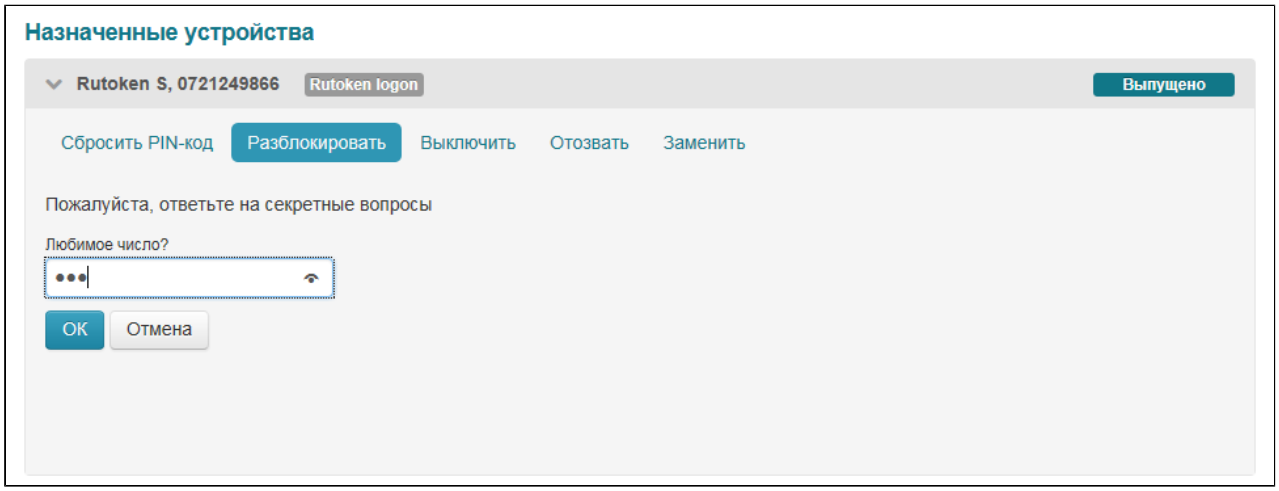
1. Онлайн-разблокировка с помощью Credential Provider.
2. Оффлайн-разблокировка с помощью утилиты разблокировки.
3. Оффлайн-разблокировка с помощью Credential Provider.

Взаимодействие с сотрудником технической поддержки требуется только в случае оффлайн-разблокировки. В этом случае пользователь на своей стороне генерирует запрос на разблокировку с помощью утилиты разблокировки или Credential Provider и связывается с сотрудником технической поддержки. Для разблокировки устройства:

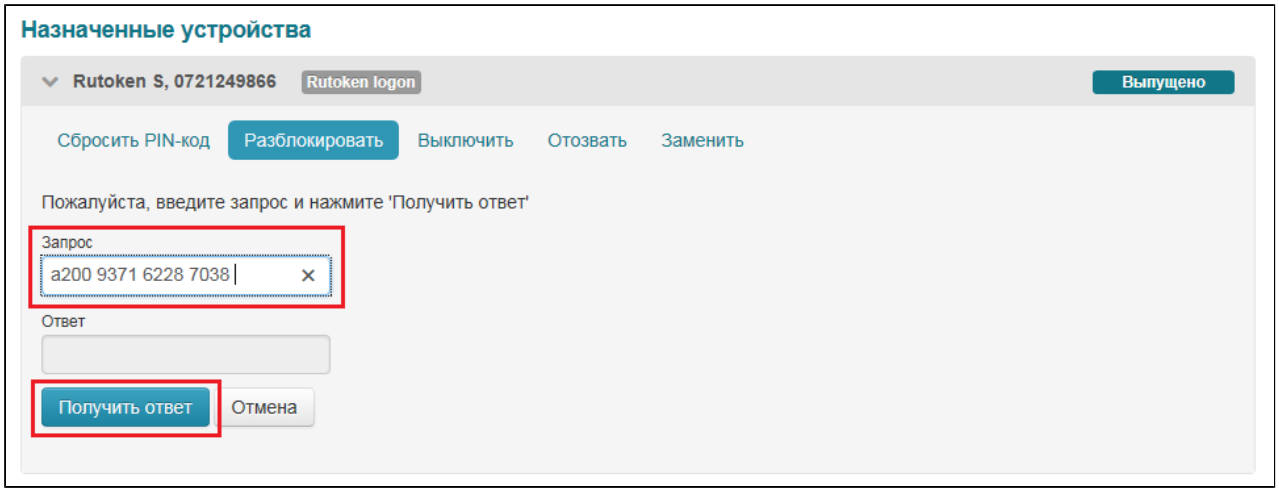
1. Перейдите в карточку пользователя, устройство которого необходимо разблокировать, выберите устройство и нажмите на ссылку **Разблокировать**:



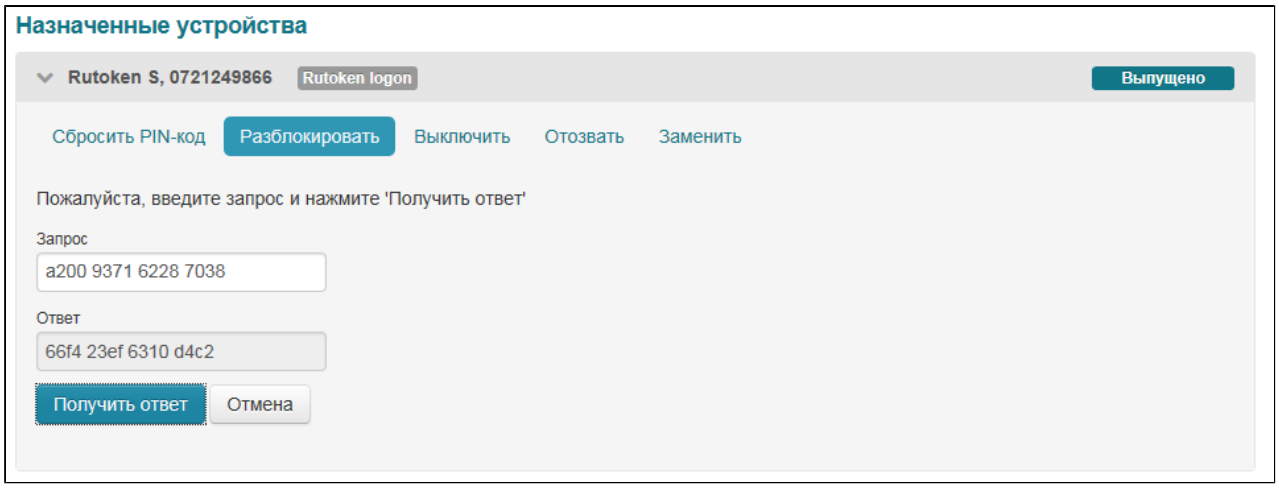
2. Запросите ответы на секретные вопросы у пользователя и введите их:



3. Введите запрос, полученный от пользователя в поле **Запрос** и нажмите на кнопку **Получить ответ**:



Сообщите сгенерированный ответ пользователю:



Дальнейшие действия по разблокировке выполняются на стороне пользователя. Для этого на компьютере пользователя должны быть установлены компоненты Client Tools. Пользователь производит разблокировку устройства с помощью Credential Provider или Rutoken KeyBox - Unblock, вводя ответ, новый PIN-код и его подтверждение. В результате устройство будет разблокировано, PIN-код Пользователя изменен.

Временное выключение

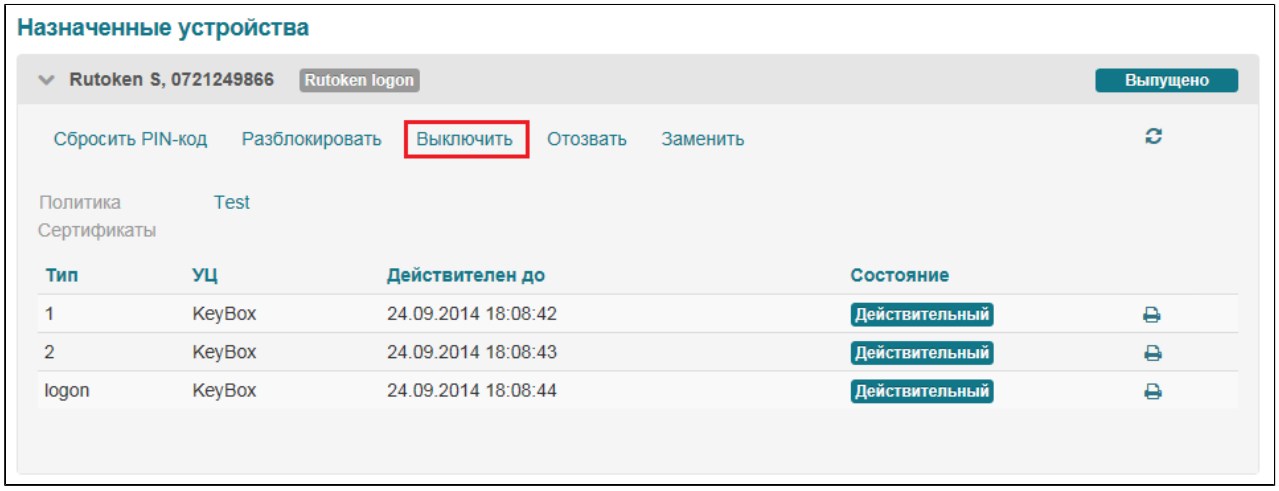
Если пользователь не планирует использовать устройство продолжительное время, например, в отпуске, то его можно временно выключить. В результате будут временно отозваны все сертификаты пользователя, хранящиеся на устройстве.

Важная информация

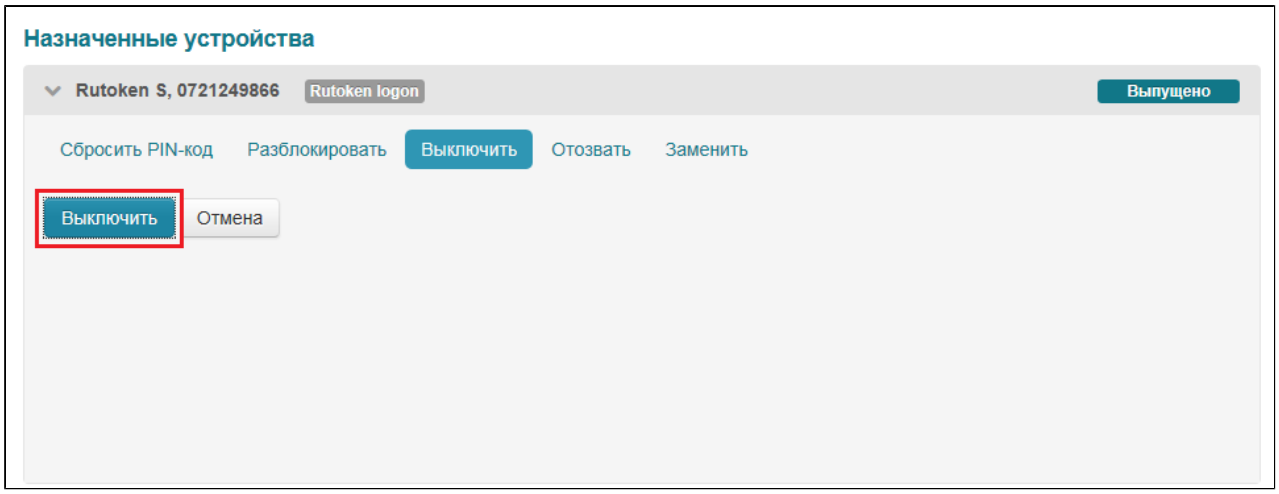
Данная операция не распространяется на сертификаты, выпущенные удостоверяющим центром КриптоПро УЦ. Их действие не будет приостановлено.

Для выключения:

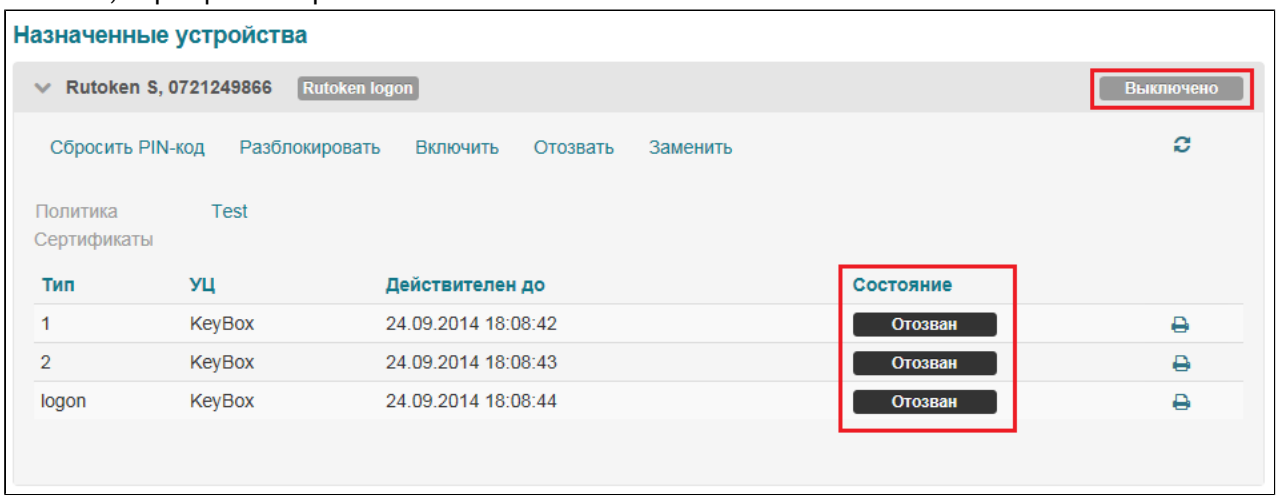
1. В карточке пользователя, устройство которого необходимо выключить, выберите устройство и нажмите на ссылку **Выключить**:



2. Подтвердите выключение, нажав на кнопку **Выключить**:

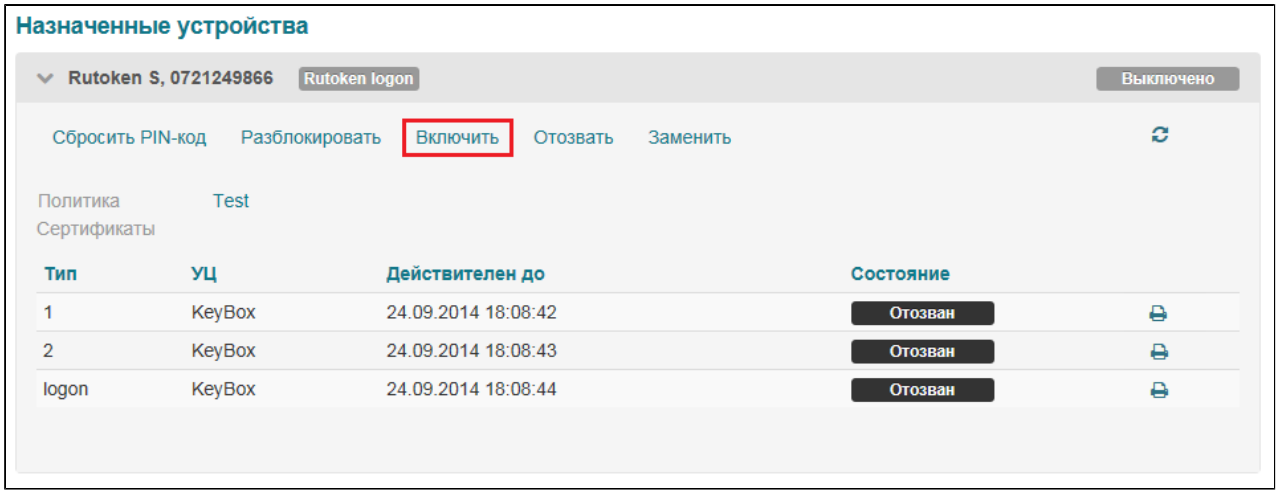


Устройство будет выключено. Статус устройства в карточке пользователя и личном кабинете будет изменен, сертификаты временно отозваны:

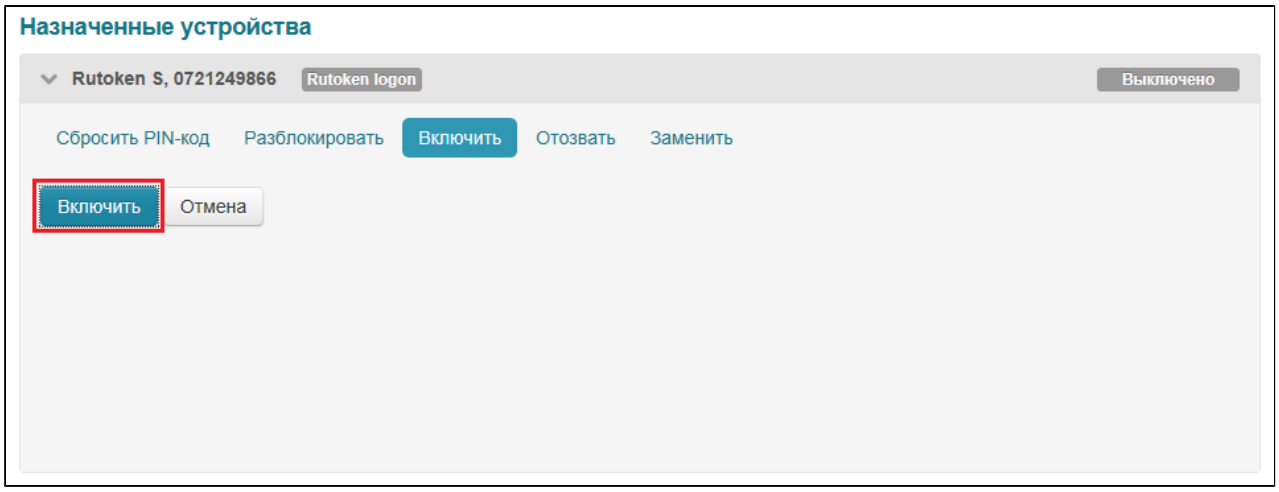


Для восстановления действия необходимо включить устройство:

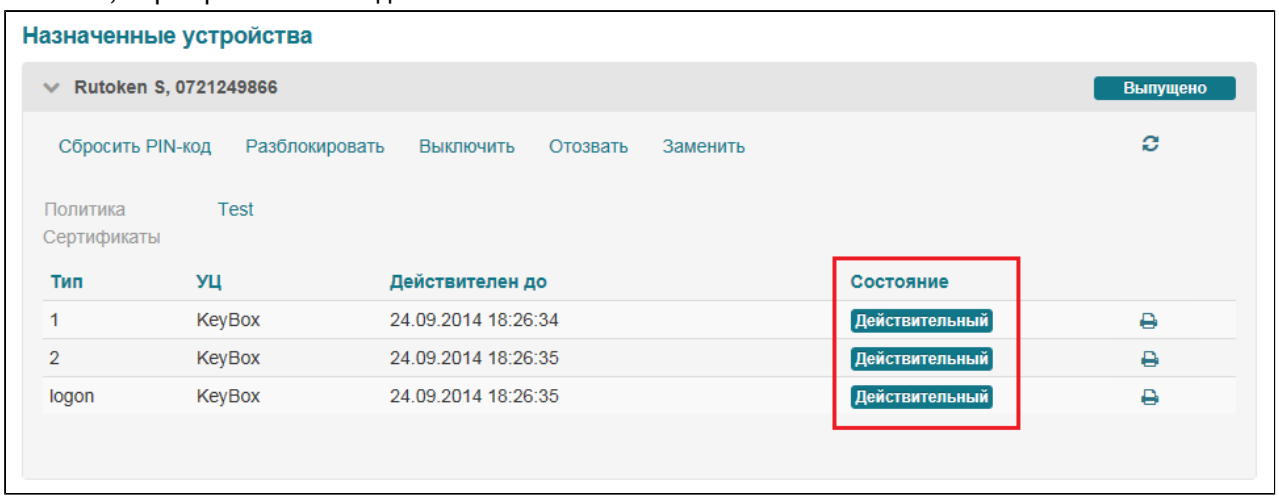
1. В карточке пользователя, устройство которого необходимо включить, выберите устройство и нажмите на ссылку **Включить**:



Подтвердите выключение, нажав на кнопку **Включить**:



Устройство будет включено. Статус устройства в карточке пользователя и личном кабинете будет изменен, сертификаты снова действительны:



Отзыв устройства

Устройство может быть отозвано в случае его утраты, поломки, обновления или необходимости удалить его из системы. При отзыве все сертификаты, хранящиеся на устройстве, будут отозваны без возможности восстановления.

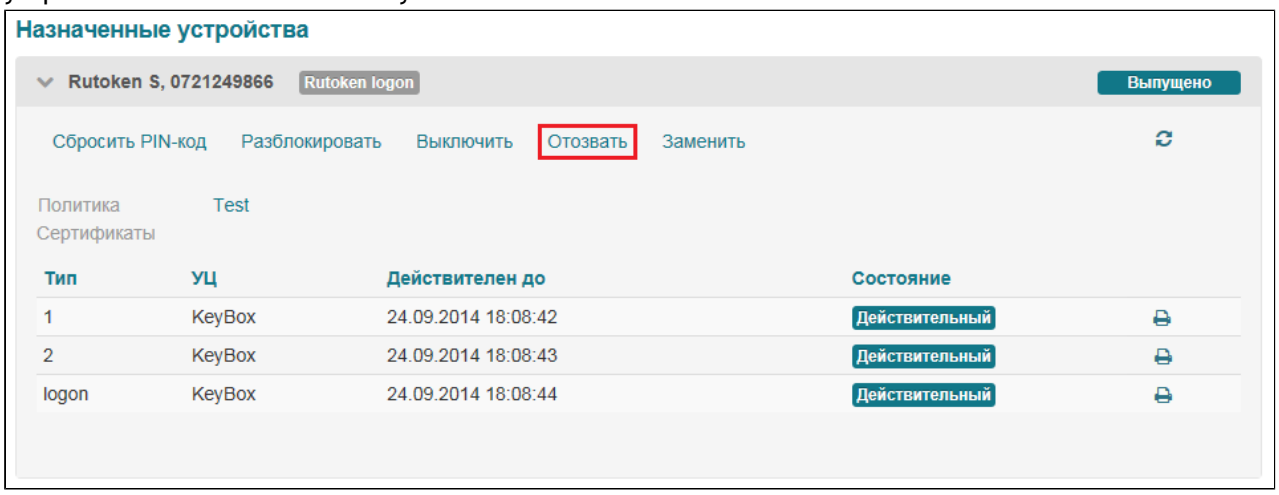
В системе предусмотрены четыре причины отзыва устройства:

1. Устройство неисправно - устройство неработоспособно по причине технической неисправности.
2. Устройство утеряно - устройство было утрачено.
3. Обновление устройства - обновление содержимого устройства в связи с изменениями в политике использования устройств в системе.
4. Изъятие устройства - удаление устройства из системы (например, при увольнении пользователя).

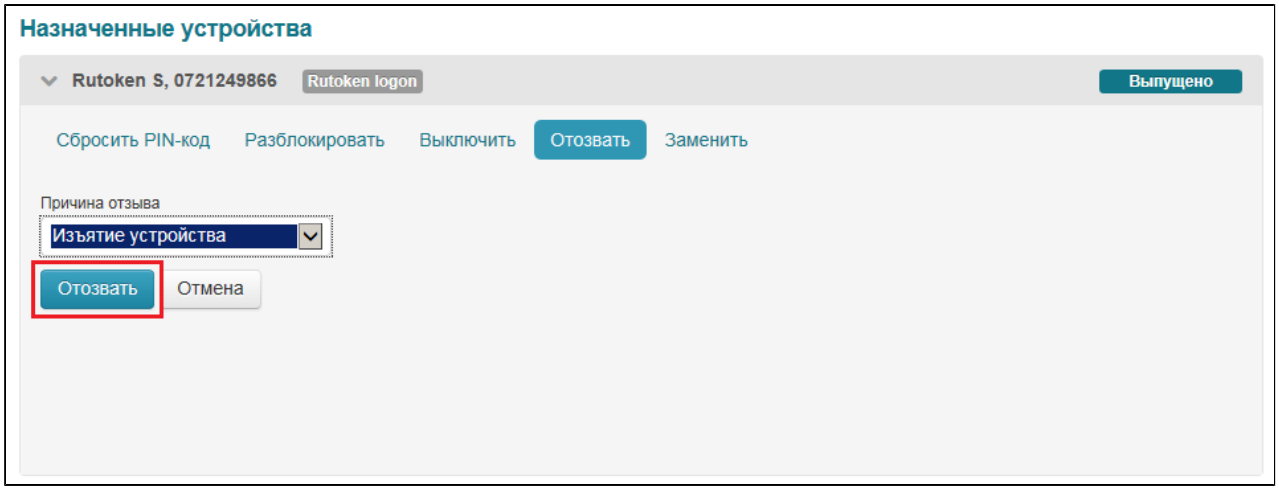
В случае отзыва устройства по причине **Устройство неисправно** или **Устройство утеряно** все сертификаты, записанные на устройство будут отозваны независимо от значения настройки политики **Отзывать сертификат при отзыве/выключении устройства**.

Для отзыва устройства:

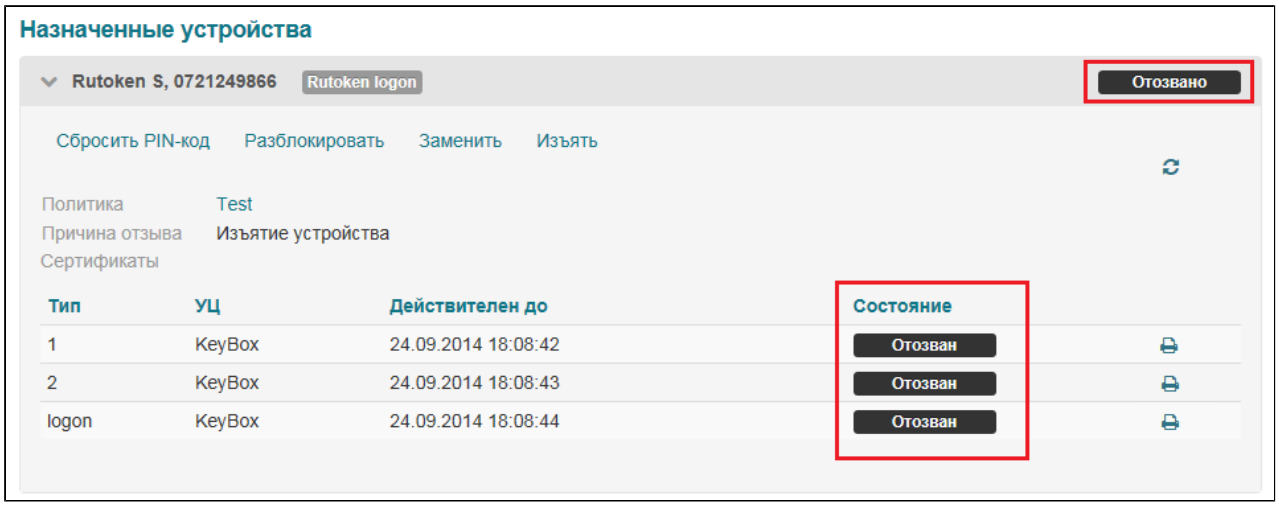
1. Перейдите в карточку пользователя, устройство которого необходимо отозвать, выберите устройство и нажмите на ссылку **Отозвать**:



2. Укажите причину отзыва и нажмите на кнопку **Отозвать**:



Устройство будет отозвано. Все сертификаты, хранящиеся на устройстве, будут отозваны без возможности восстановления. После отзыва можно произвести изъятие устройства у пользователя.

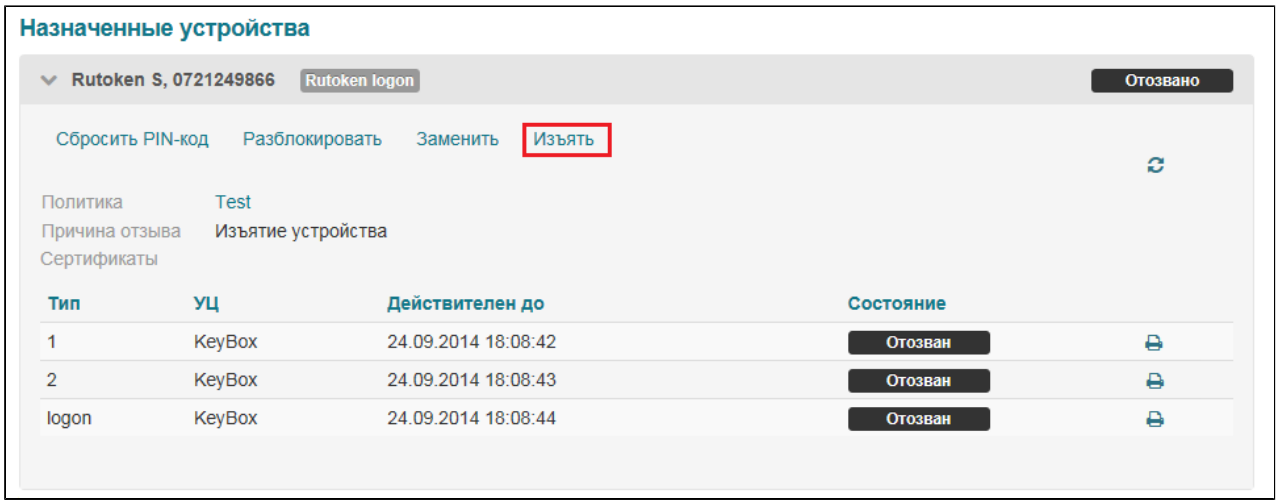


Изъятие устройства

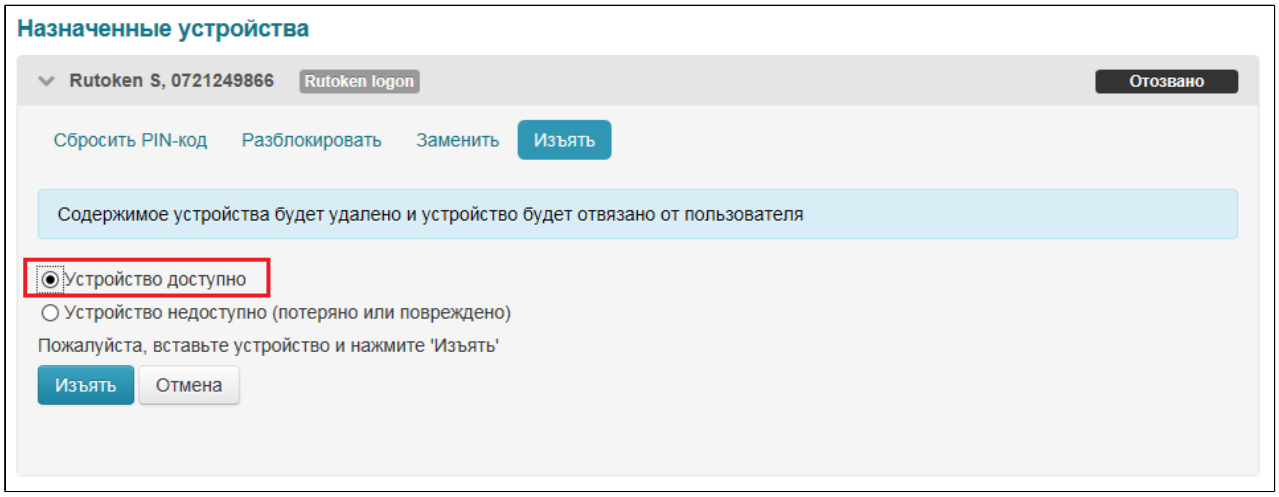
После отзыва можно изъять устройство у пользователя. В процессе изъятия происходит отмена назначения устройства. Устройство больше не привязано к конкретному пользователю. Возможно назначение его новому пользователю или полное удаление из системы.

Для изъятия устройства:

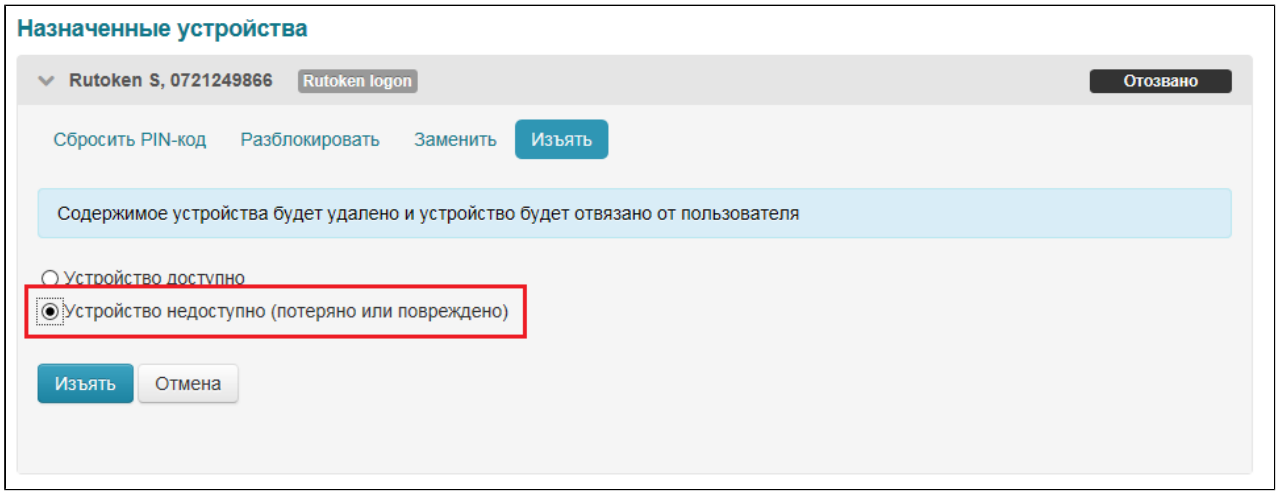
1. Перейдите в карточку пользователя, устройство которого необходимо изъять, выберите устройство и нажмите на ссылку **Изъять**:



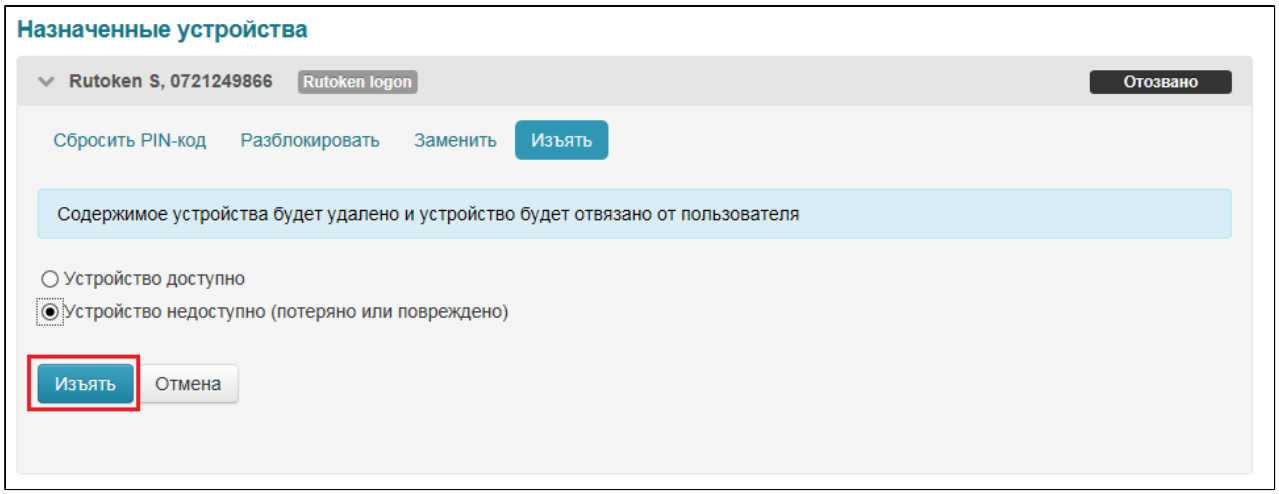
2. Выберите пункт **Устройство доступно**, если устройство есть в наличии. В этом случае из памяти устройства будет удалена вся информация, записанная в нее системой, и отменено назначение устройства пользователю.



Выберите пункт **Устройство недоступно (потеряно или повреждено)**, если устройство физически недоступно. В этом случает будет отменено назначение устройства пользователю.



3. Нажмите на кнопку **Изъять**:



Устройство будет изъято.

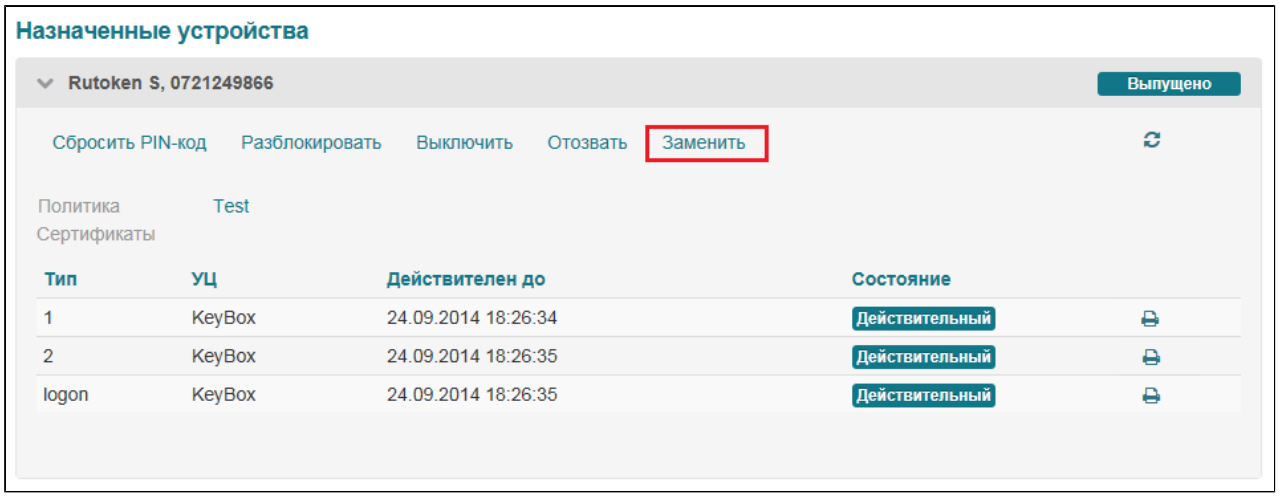
Замена устройства

Замена предполагает запись действующих сертификатов и ключевой информации на новое устройство. В системе предусмотрено два типа замены устройств:

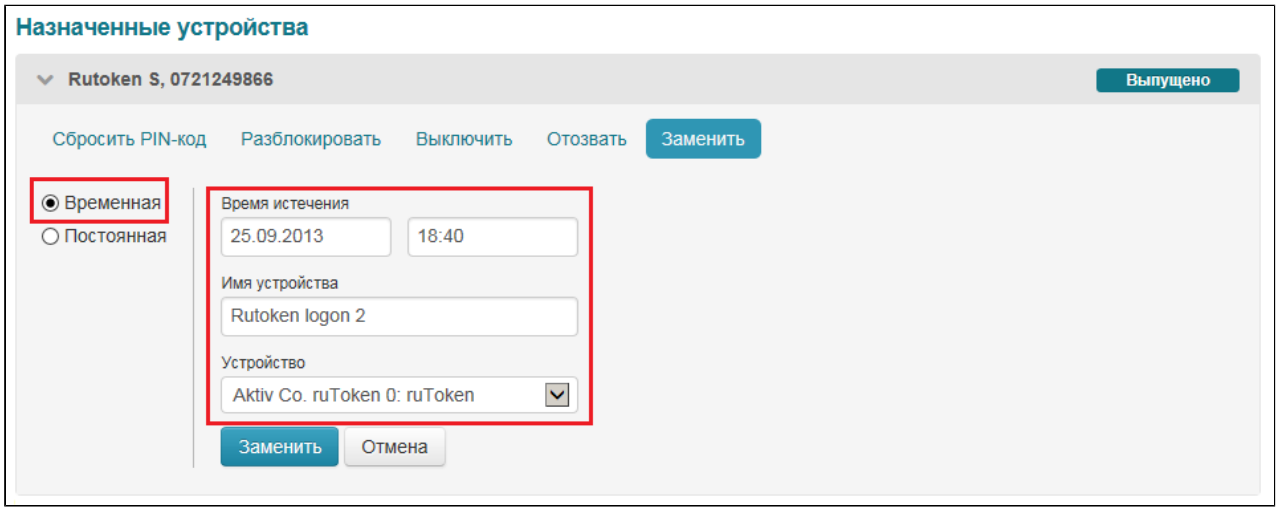
1. Временная замена. Предусмотрена на случай, когда устройство временно недоступно (например, если сотрудник забыл устройство дома). При временной замене пользователю будет выдано новое устройство с ограниченным сроком действия. Основное устройство пользователя будет временно выключено, сертификаты на нем - временно отозваны.
2. Постоянная замена. Предусмотрена на случай утраты основного устройства пользователя. В случае постоянной замены сертификаты, хранящиеся на основном устройстве пользователя будут отозваны без возможности восстановления. Действующие сертификаты и ключевые пары будут записаны на новое устройство.

Для замены устройства:

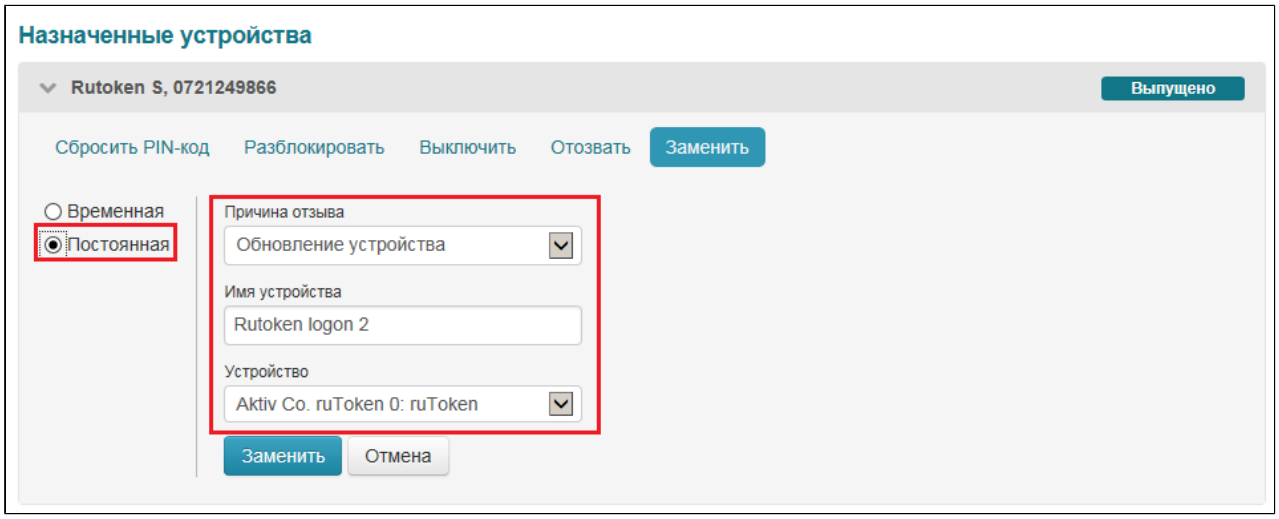
1. Перейдите в карточку пользователя, устройство которого необходимо заменить, выберите устройство и нажмите на ссылку **Заменить**:



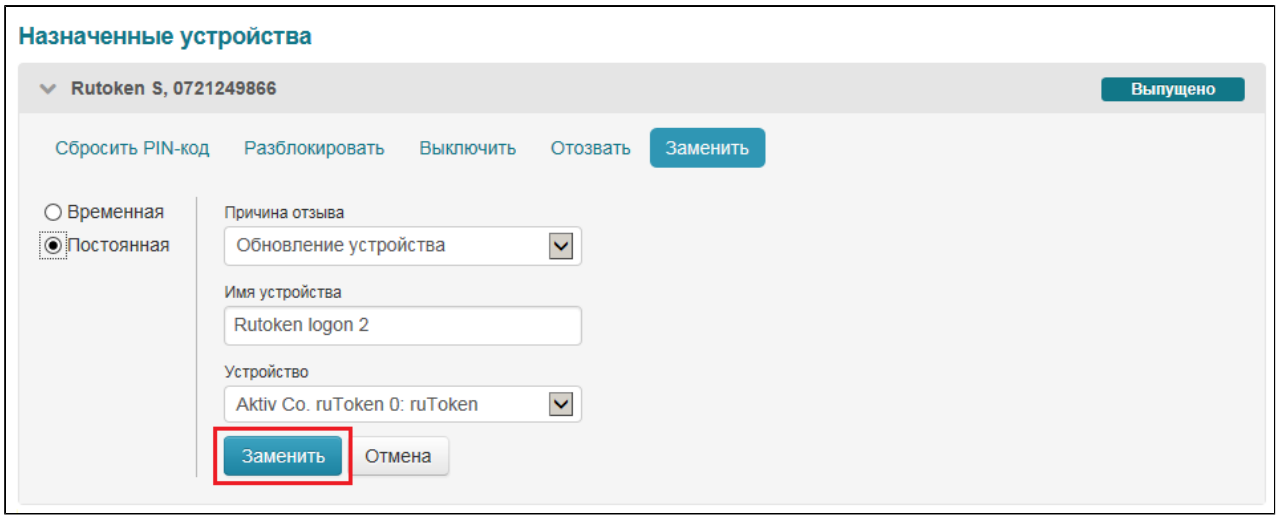
2. Подключите новое устройство.
3. Выберите тип замены. Для временной замены укажите время истечения срока действия устройства, новое имя устройства и выберите из списка новое устройство:



Для постоянной замены укажите причину замены, новое имя устройства и выберите из списка новое устройство:



4. Нажмите на кнопку **Заменить**:



Обновление устройства

В случае если срок действия одного или нескольких сертификатов истек, сотрудник технической поддержки может обновить сертификаты без перевыпуска устройства. Обновление так же доступно, если в политику были добавлены новые шаблоны сертификатов.

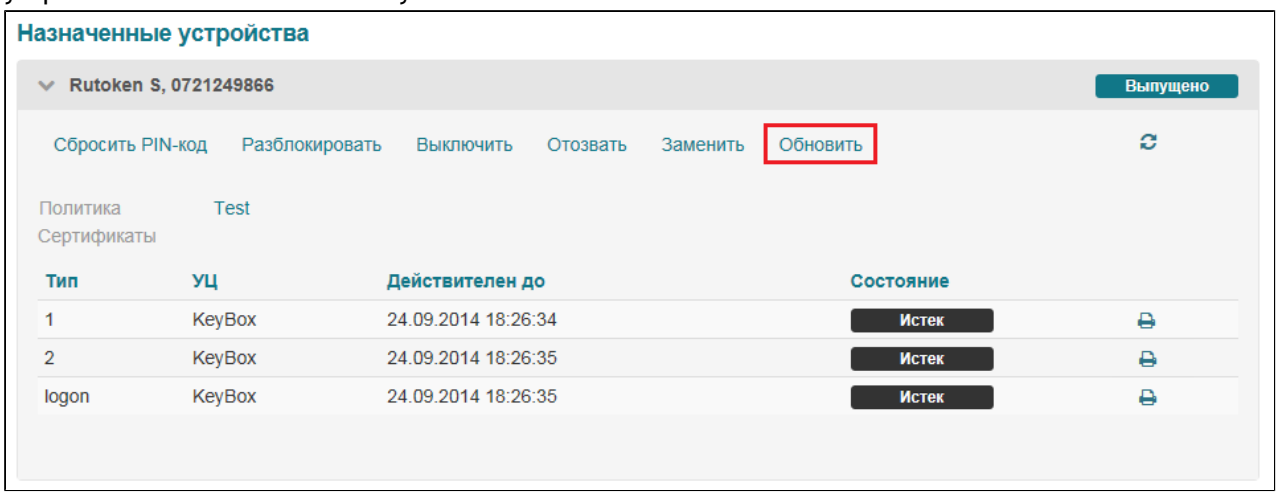
Важная информация

Операция обновления недоступна, если были внесены изменения в текущие шаблоны сертификатов политики.

Обновление устройства доступно так же в личном кабинете пользователя.

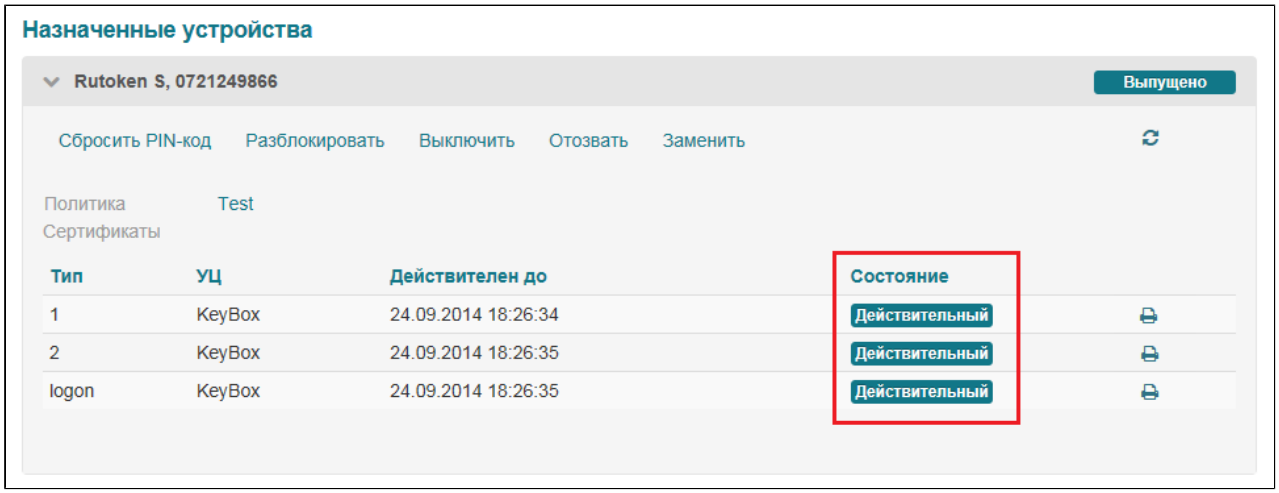
Для обновления устройства:

1. Перейдите в карточку пользователя, устройство которого необходимо обновить, выберите устройство и нажмите на ссылку **Обновить**:



2. Введите PIN-код Пользователя и нажмите на кнопку **Обновить**:

Сертификаты на устройстве будут обновлены.

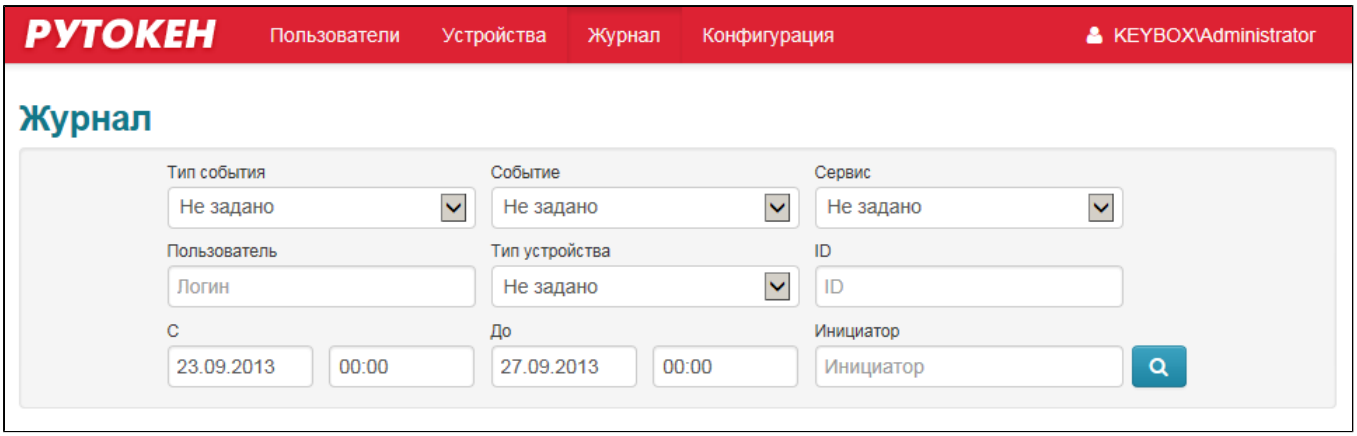


Журнал

Записи обо всех операциях приложений Management Console, Self Service, Remote Self Service отражаются в журнале событий. Раздел **Журнал** предназначен для поиска и просмотра информации о событиях в системе.

События системы делятся на несколько типов:

Тип события	Обозначение	Описание
Информация		Успешное выполнение любой операции в системе.
Предупреждение		События, требующие внимания администратора системы.
Ошибка		Завершение операции с ошибкой.

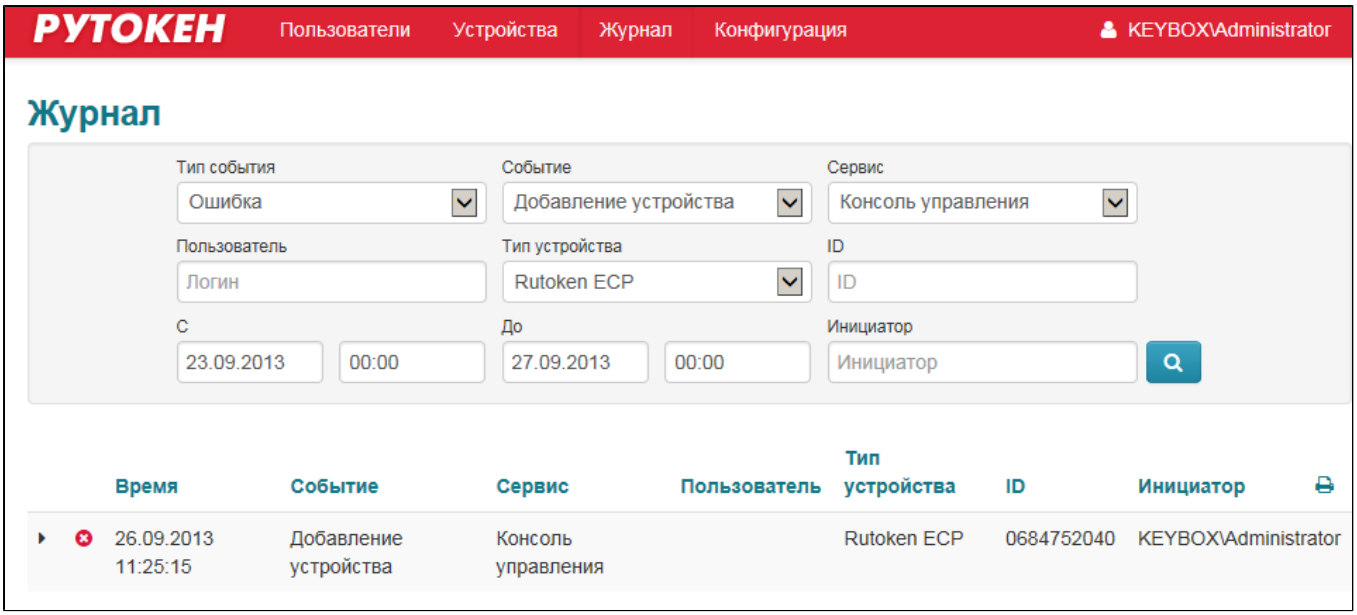


Поиск событий в журнале осуществляется по следующим параметрам:

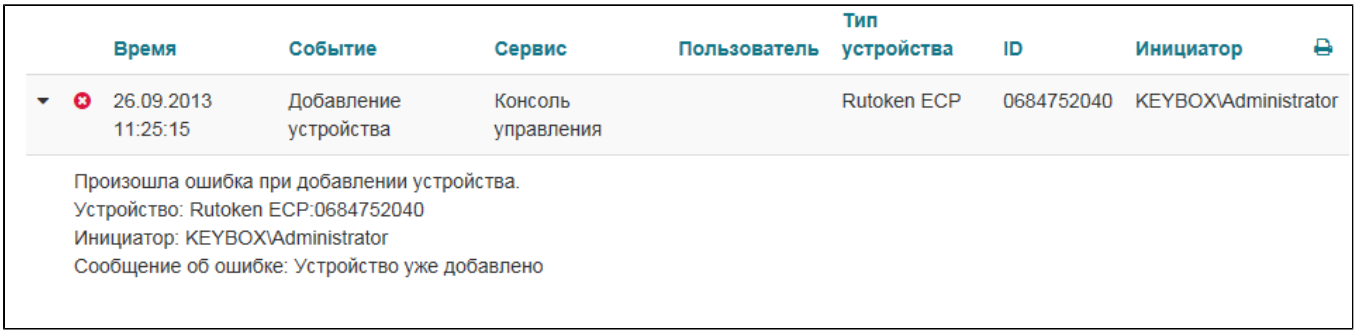
Параметр	Описание
Тип события	Тип события: информация, предупреждение или ошибка
Событие	Действие, выполненное в системе
Сервис	Часть системы, с помощью которой действие было произведено
Пользователь	Пользователь, с учетной записью или устройством которого было произведено действие. Данный параметр может присутствовать не для всех событий
Тип устройства	Тип устройства, с которым было произведено действие. Список строится на основе типов устройств в разделе Конфигурация. Данный параметр может присутствовать не для всех событий
ID	ID устройства, с которым было произведено действие. Данный параметр может присутствовать не для всех событий
С... до...	Период времени
Инициатор	Пользователь, инициировавший событие

Для поиска событий в журнале заполните все необходимые поля и нажмите на кнопку  .

В таблице будут выведены все события, соответствующие критериям поиска:



Для просмотра более подробной информации об ошибке нажмите на пиктограмму :



Для сброса результатов поиска обновите страницу.

Раздел 4. Руководство пользователя системы

Личный кабинет пользователя

Для управления персональными устройствами аутентификации пользователей в системе Рутокен KeyBox реализован личный кабинет пользователя - Self Service.

Личный кабинет пользователя используется для решения следующих задач:

- Выпуск устройства
- Выключение устройства
- Включение устройства
- Отзыв устройства
- Изменение/сброс PIN-кода устройства
- Обновление содержимого устройства
- Установка секретных вопросов
- Изменение ответов на секретные вопросы.

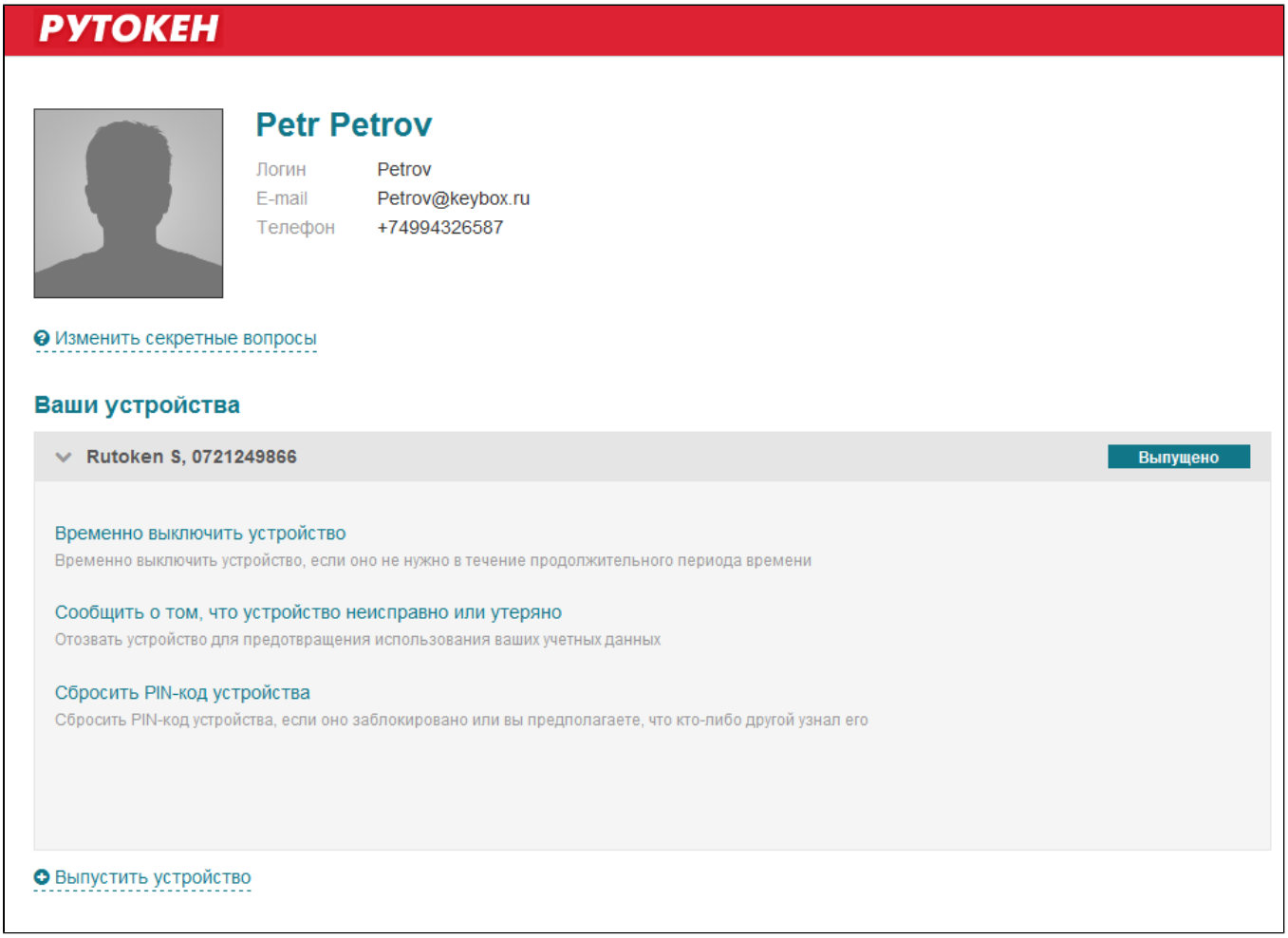
Личный кабинет представляет собой Web-приложение. Для доступа к приложению Self Sevice необходимо открыть браузер и в адресной строке ввести: https://адрес сервера Рутокен KeyBox/**keyboxservice** /

Важная информация

Для доступа к Личному кабинету необходимо использовать браузер Internet Explorer 8 и выше.

Вход в систему

В зависимости от типа контроля доступа возможно два варианта аутентификации в системе:
1. Аутентификация Windows. Дополнительные действия не требуются, пройдя аутентификацию в домене пользователь получает доступ к сервисам системы.
2. Аутентификация по сертификатам. Для получения доступа к сервисам системы необходимо подключить токен с соответствующим сертификатом.



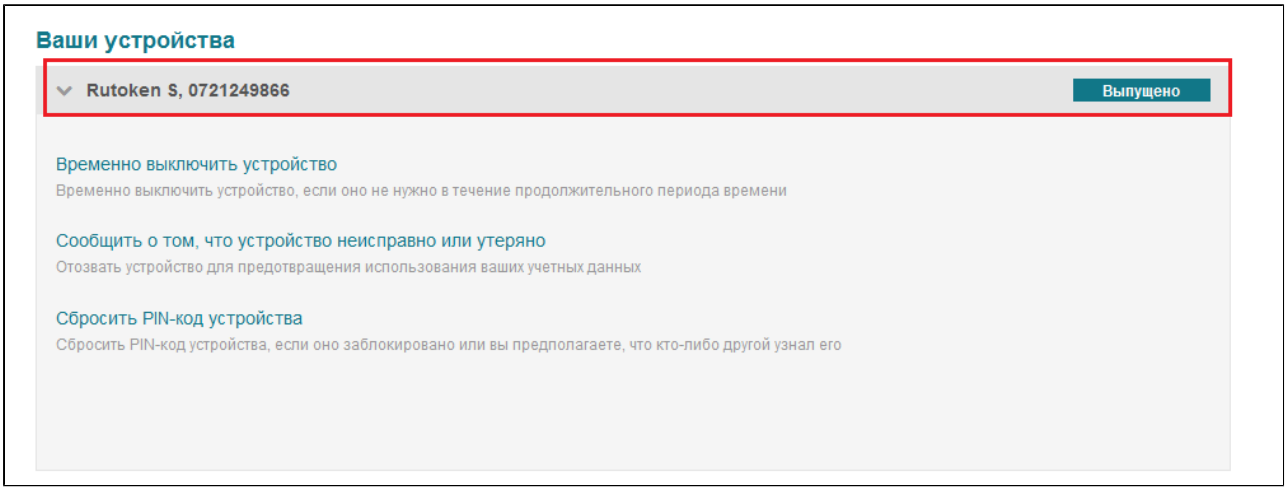
Важная информация

Если Вы не можете войти в приложение, обратитесь к администратору.
Набор действий, доступных пользователю в приложении Self Service , определяется администратором системы. В данном руководстве описаны все возможные действия, доступные пользователю.

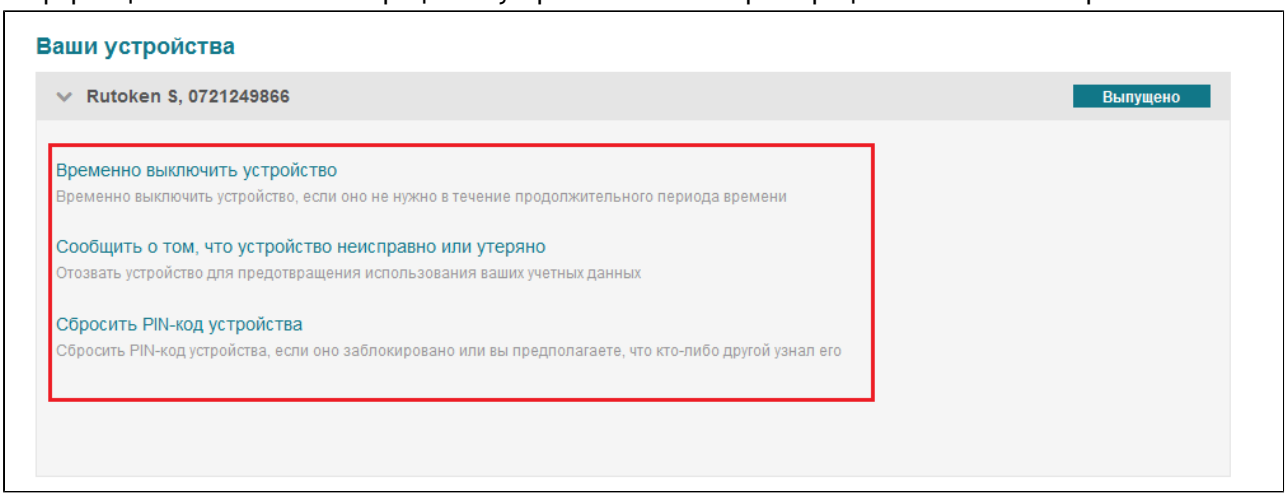
В Self Service содержится следующая информация:

- Информация о пользователе: логин пользователя, e-mail, номер телефона.

- Информация об устройствах пользователя. Список назначенных пользователю устройств с указанием типа устройства, ID, имени устройства (если оно было задано), состояние устройства.



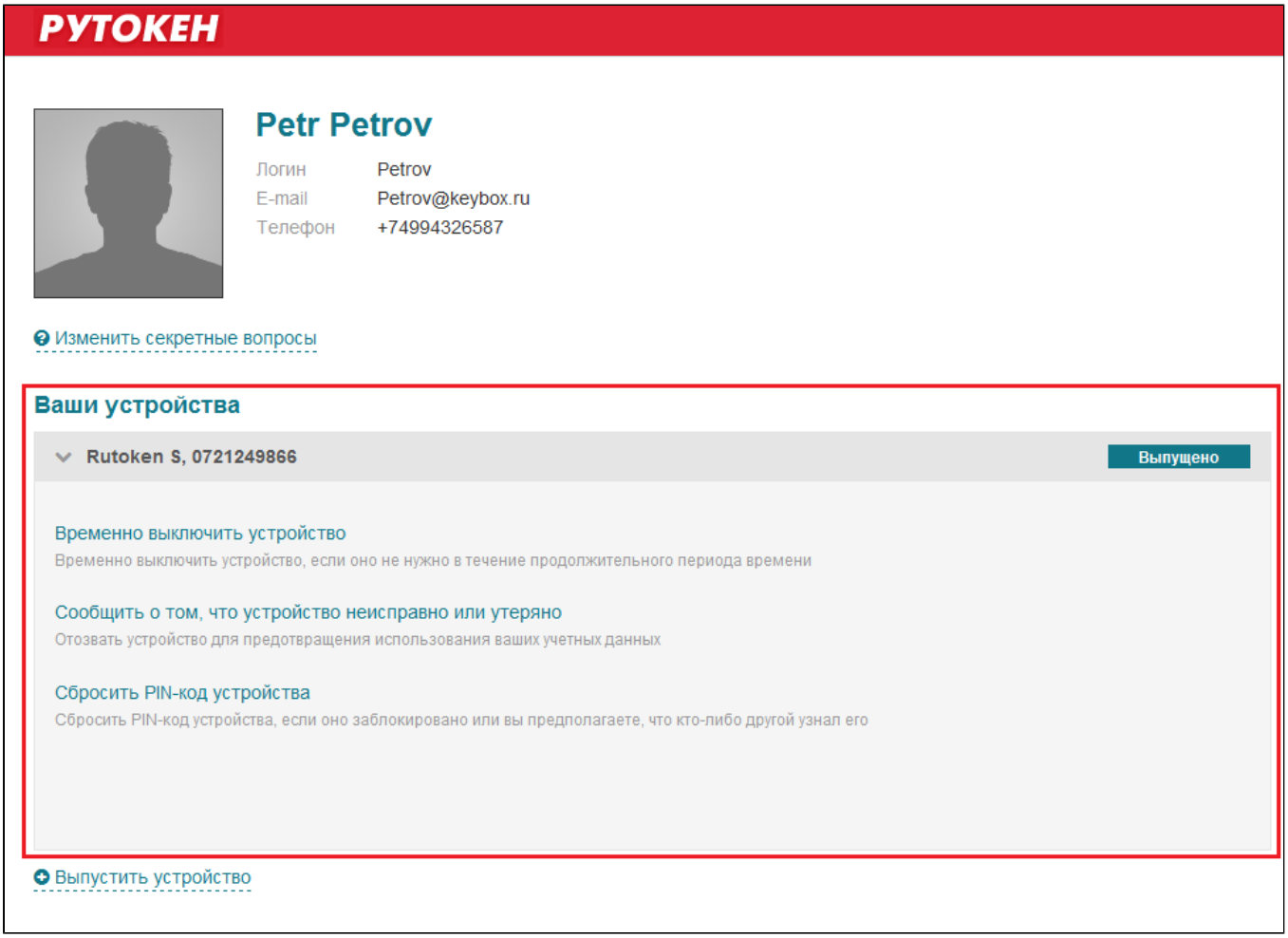
- Информация о возможных операциях с устройствами. Набор операций зависит от настроек системы.



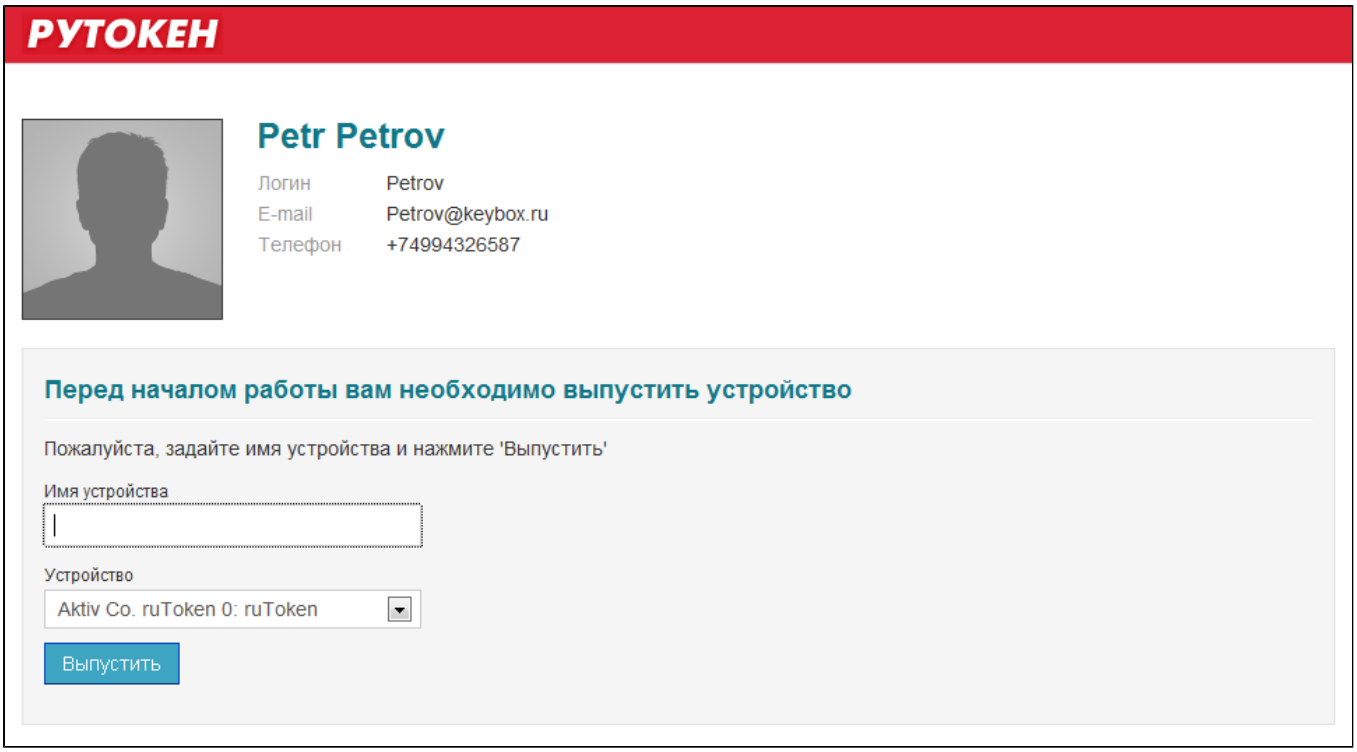
Выпуск устройства

Вы можете получить уже готовое к работе устройство у оператора службы поддержки или администратора системы, либо выпустить его самостоятельно, получив “чистое” устройство у оператора службы поддержки.

Если устройство зарегистрировано в системе и готово к работе, то при входе в приложение Self Service отобразится информация о нем:

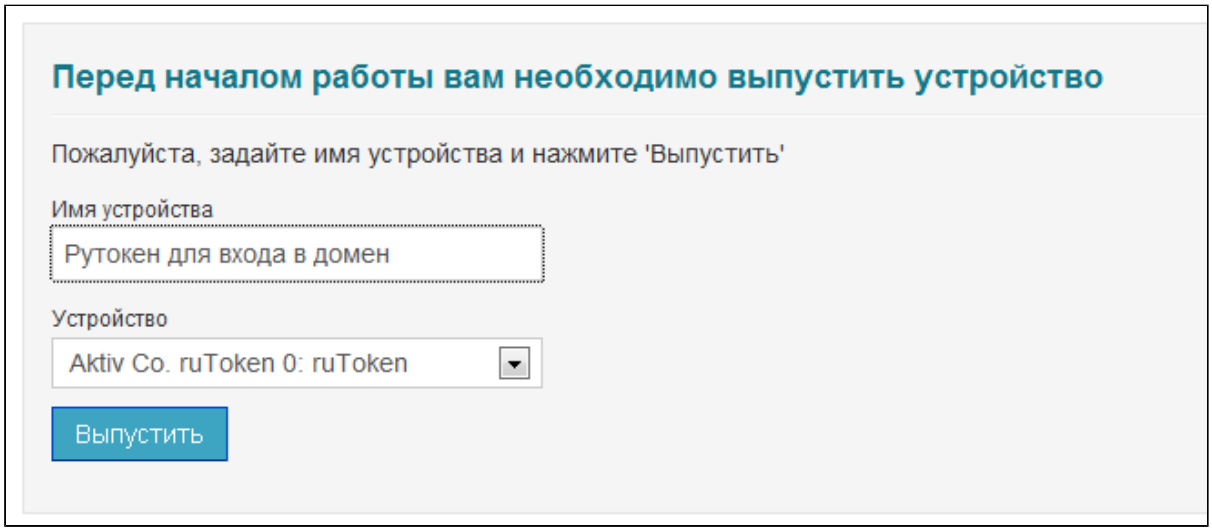


Если предполагается самостоятельный выпуск устройства, то при входе в приложение Self Service запустится мастер выпуска:

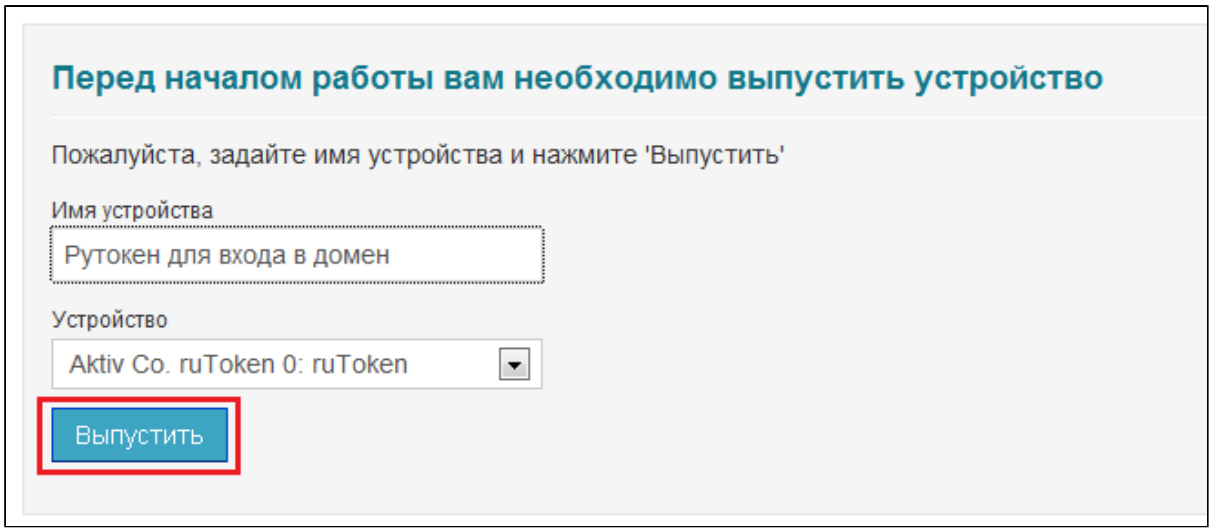


Для выпуска выполните следующие действия:

1. Подключите устройство к компьютеру и дождитесь его появления в поле устройство, задайте имя устройства. Например, “Рутокен для входа в домен”:



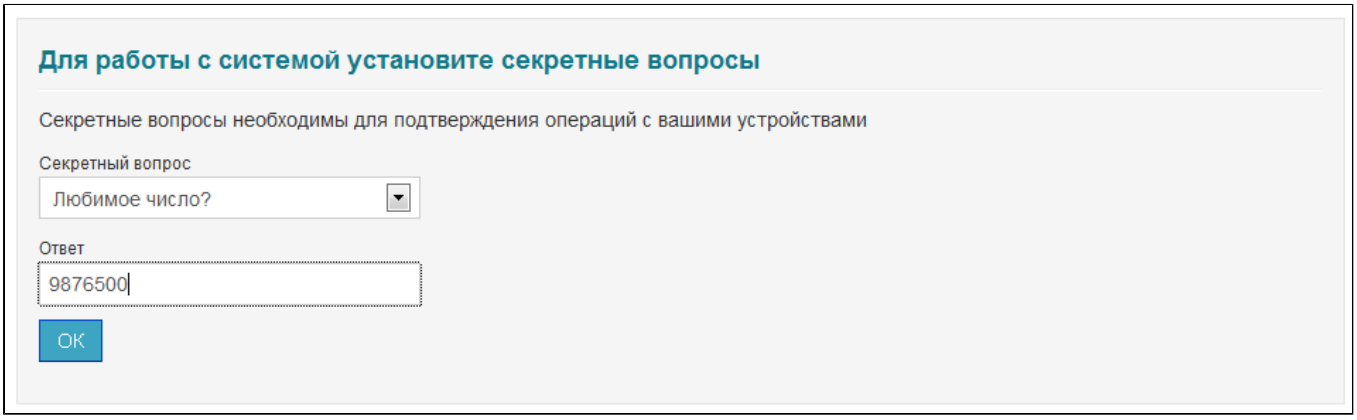
2. Нажмите Выпустить:



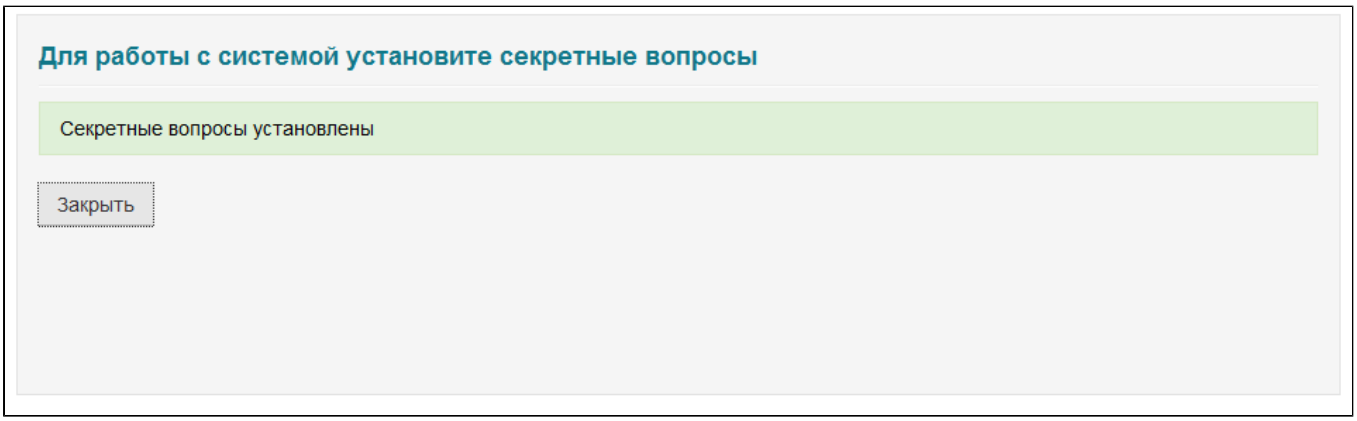
Важная информация

Если администратором включена опция инициализации устройства, то в процессе выпуска все данные, хранящиеся на нем, будут удалены.

3. Задайте секретные вопросы и ответы на них, если система запросит это, и нажмите на кнопку **ОК**:



4. Нажмите на кнопку **Закрыть** для продолжения работы с системой:

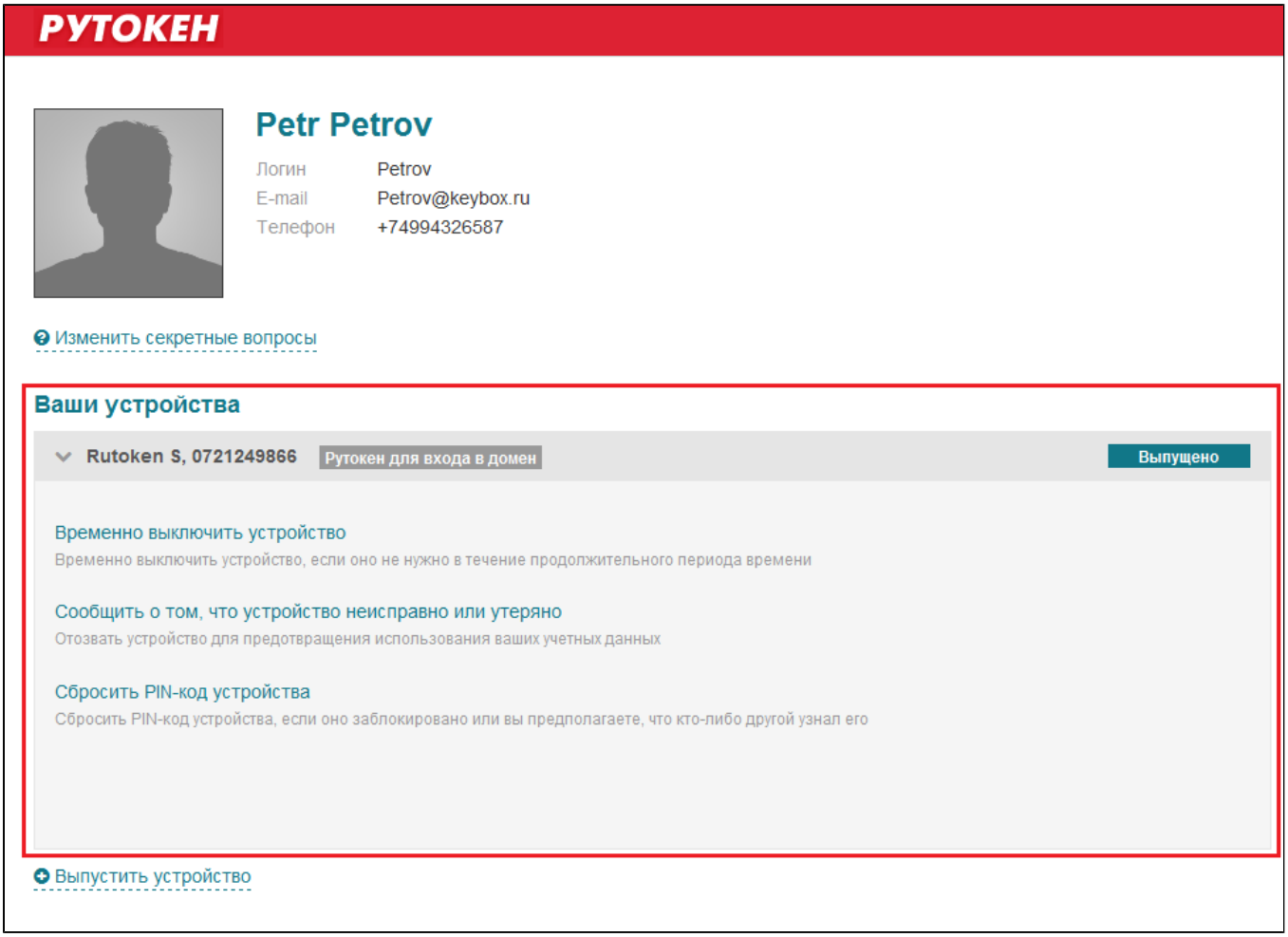


Важная информация

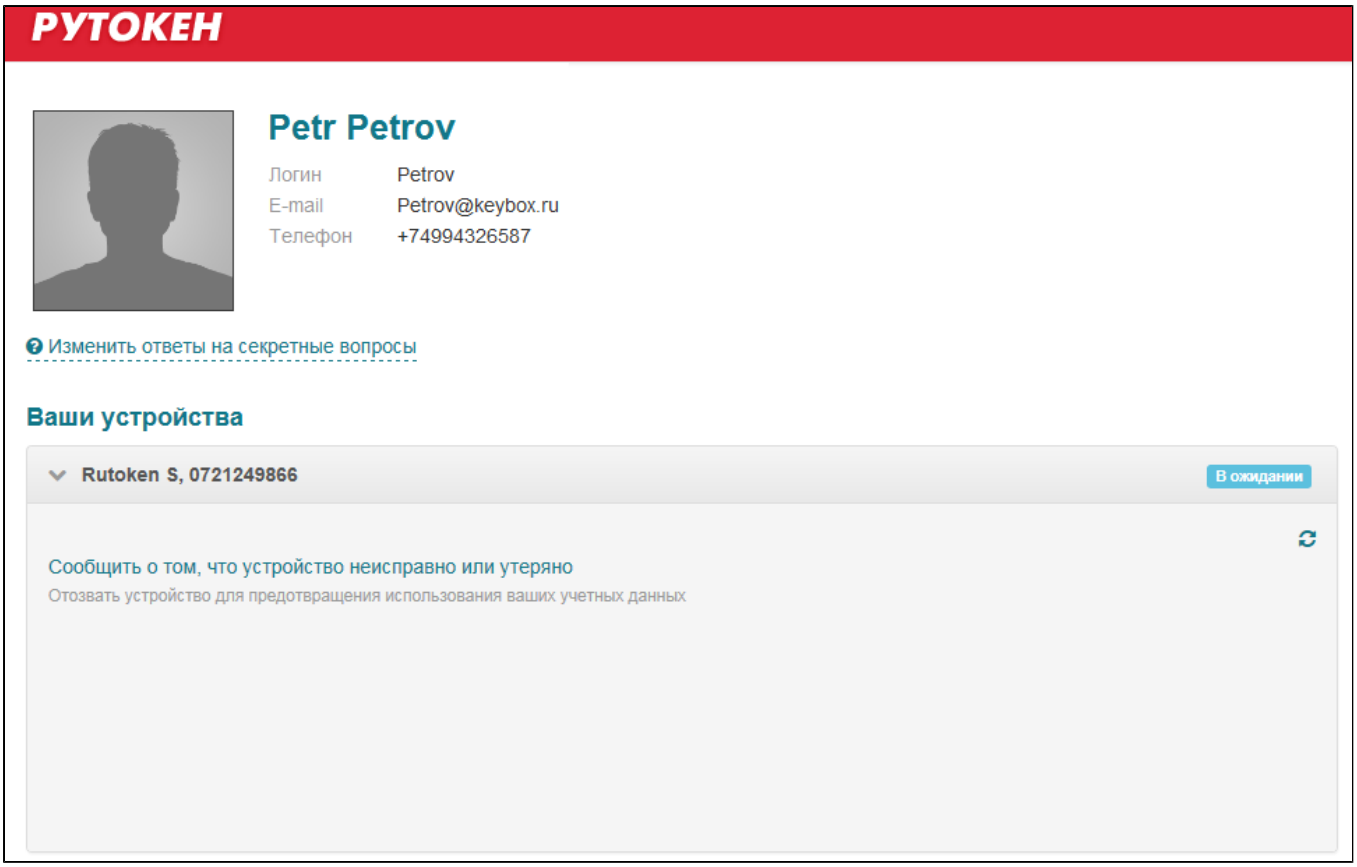
Количество вопросов при выпуске устройства задается администратором системы.

После выпуска появится раздел **Ваши устройства** , где будут сведения о выпущенном устройстве :

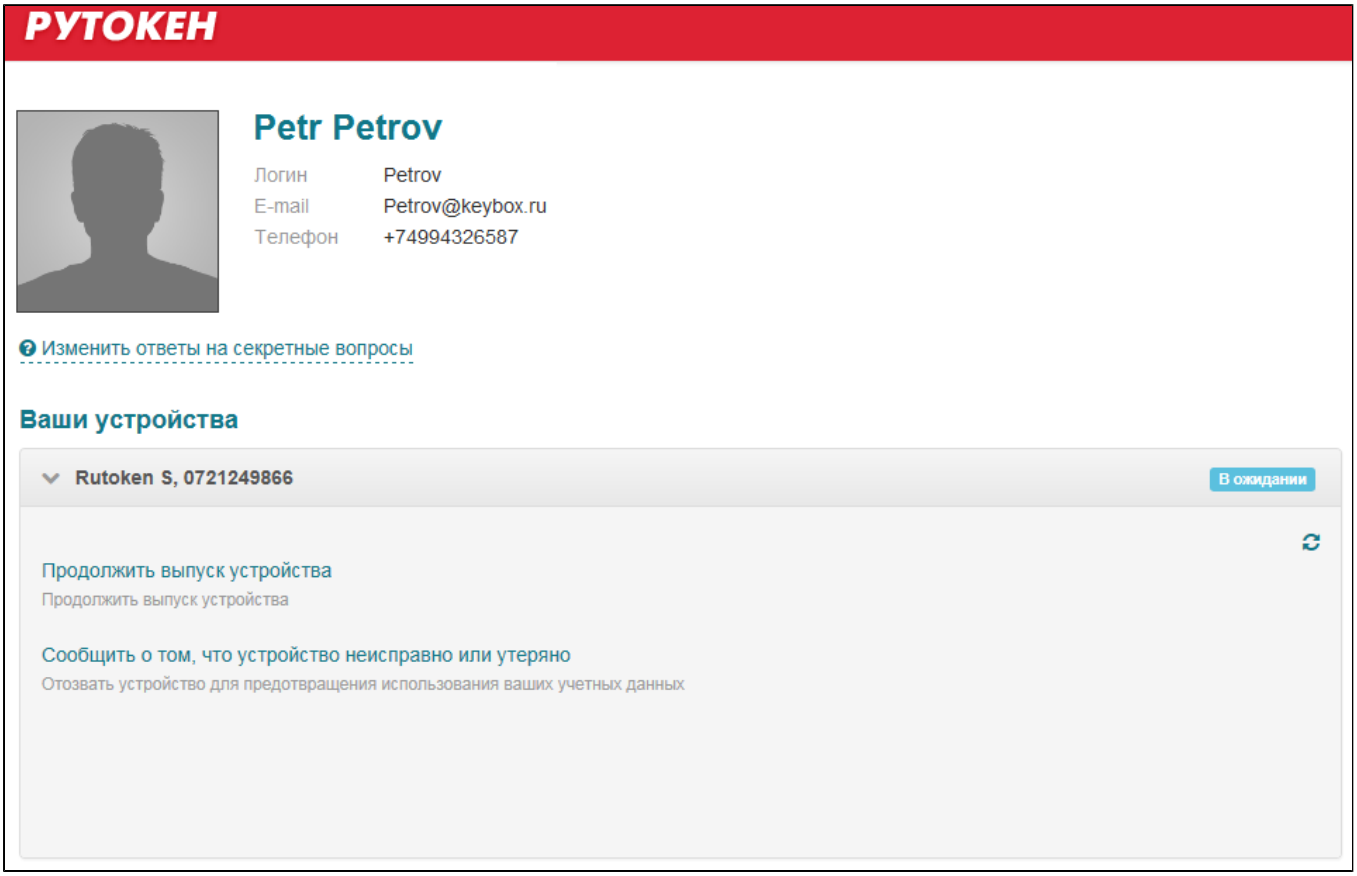
- Тип
- Серийный номер
- Имя
- Статус



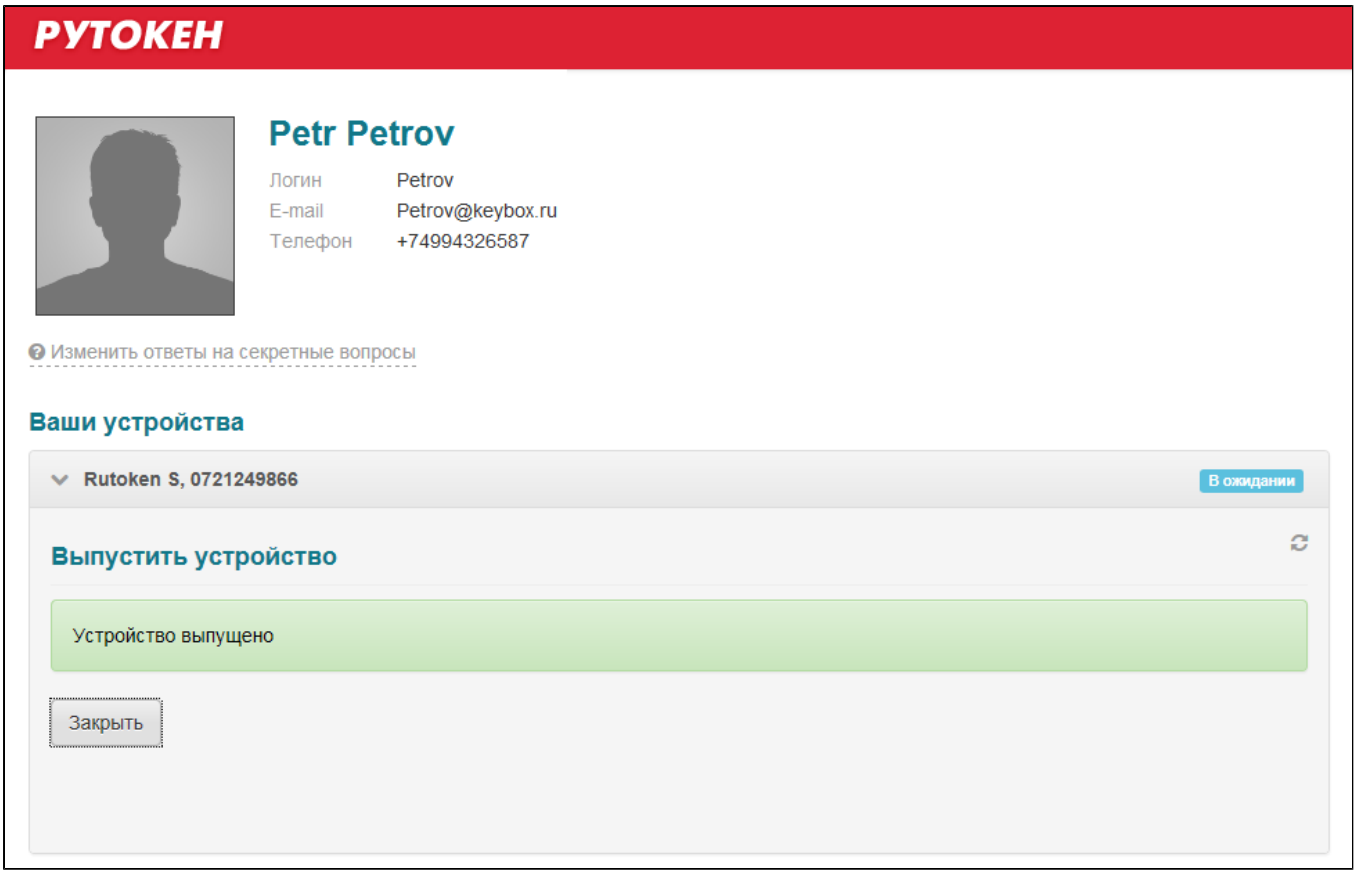
Если политикой безопасности предприятия предусмотрено подтверждение запросов на сертификат, то устройство будет находится в состоянии **В ожидании** до тех пор, пока запрос не будет одобрен. До завершения выпуска работа с ним невозможна. Сеанс работы с личным кабинетом может быть завершен, устройство можно отключить от компьютера.



После одобрения запроса на сертификат можно завершить выпуск устройства для этого нажмите на ссылку **Продолжить выпуск устройства**:



После этого устройство будет готово к работе:



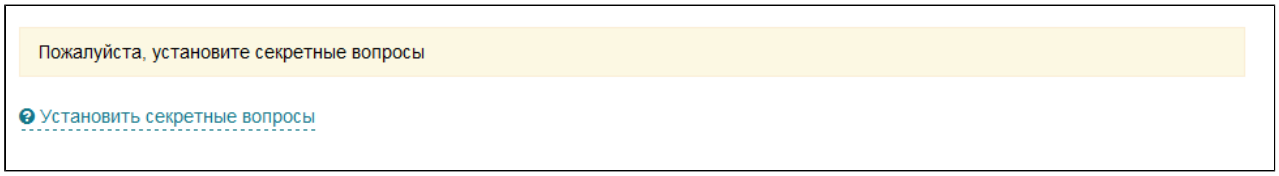
Важная информация

Секретные вопросы являются обязательными для проведения процедуры разблокировки устройства и доступа к удаленному личному кабинету пользователя (Remote Self Service), который позволяет отзывать устройства и разблокировать PIN-код за пределами домена. Если они не заданы, то эти действия будут недоступны.

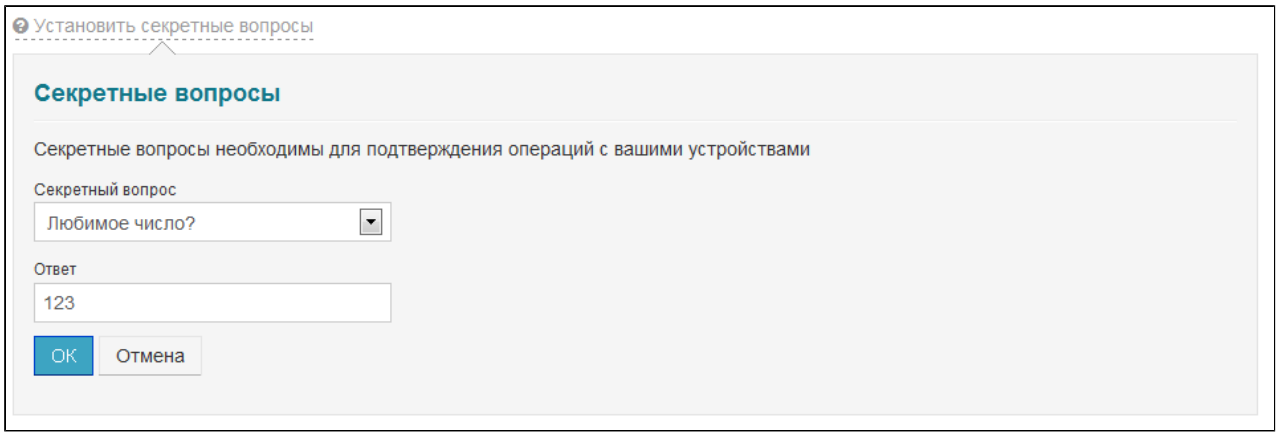
Если секретные вопросы не были заданы при выпуске, перейдите к установке секретных вопросов.

Чтобы установить секретные вопросы:

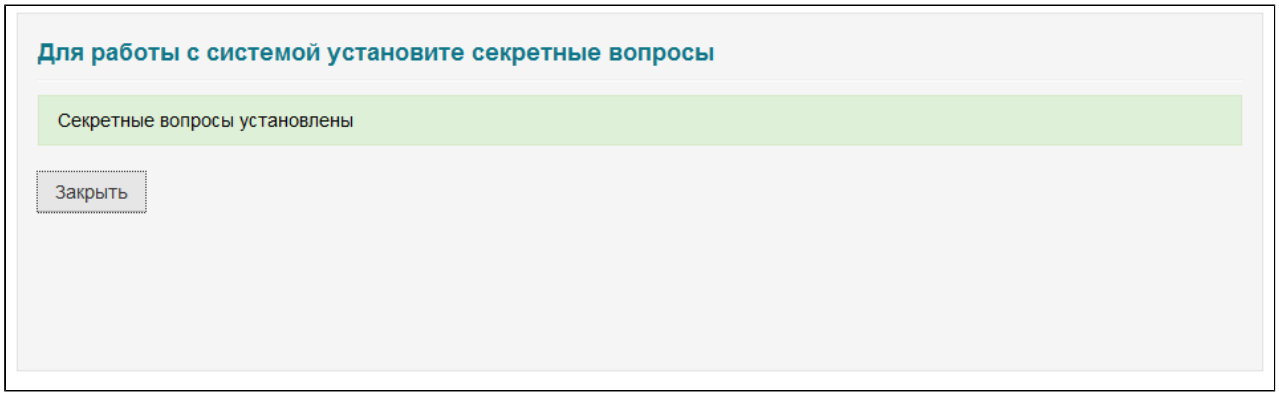
1. Нажмите **Установить секретные вопросы** в Карточке пользователя:



2. Выберите вопрос из списка доступных и задайте на него ответ:



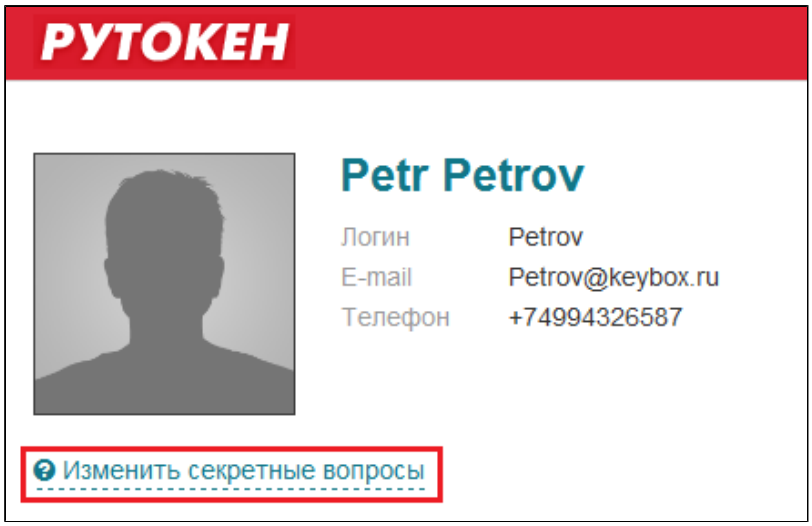
3. Нажмите **ОК** для сохранения изменений .
4. Нажмите на кнопку **Закрыть** для продолжения работы с системой:



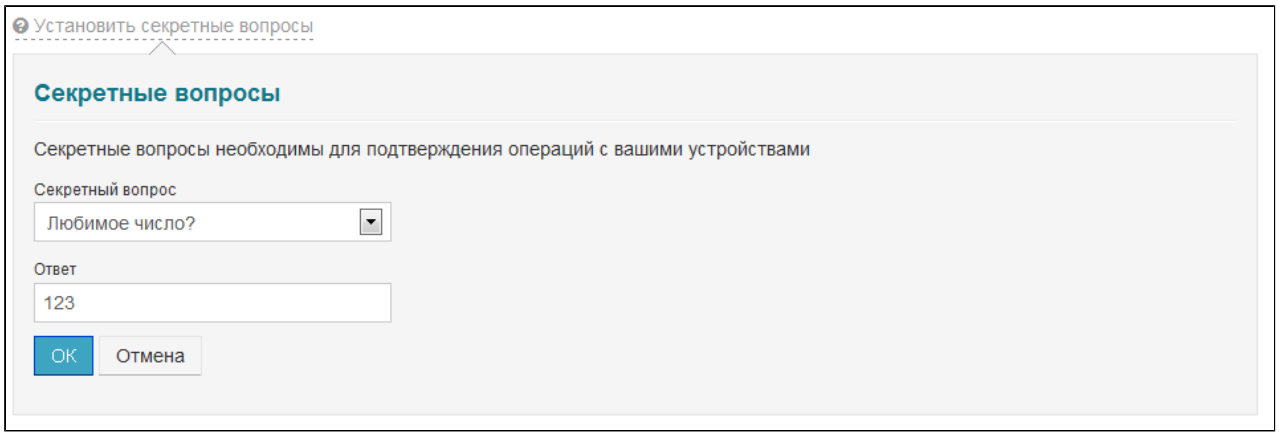
Изменение секретных вопросов

Чтобы изменить секретные вопросы:

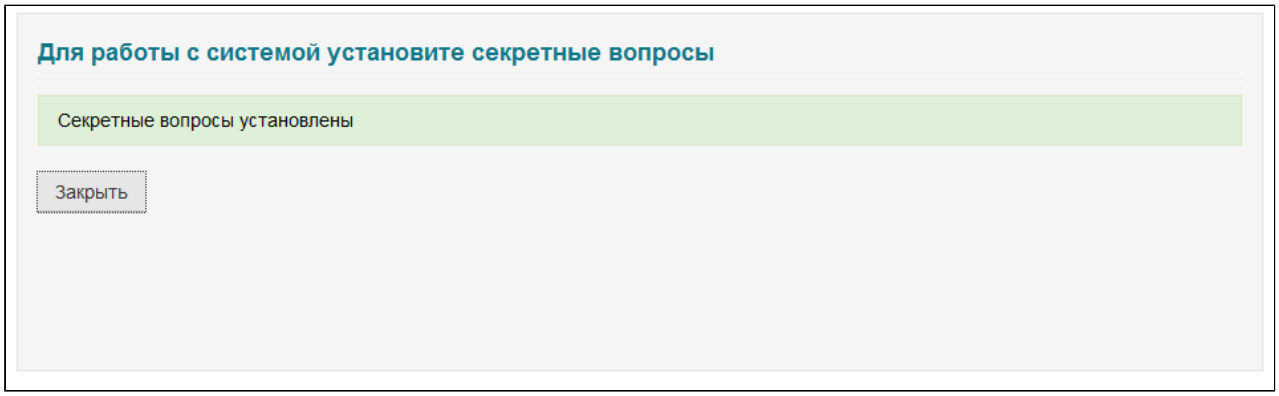
1. Нажмите **Изменить секретные вопросы** в Карточке пользователя:



2. Выберите вопрос из списка доступных и укажите ответ на него:



3. Нажмите **ОК** для сохранения изменений .
4. Нажмите на кнопку **Закрыть** для продолжения работы с системой:



Важная информация

Если ответы на секретные вопросы были забыты, то изменить их можно только связавшись с администратором системы.

Выключение устройства

Если устройство не будет использоваться продолжительное время, например, в период отпуска,то его можно временно отключить.

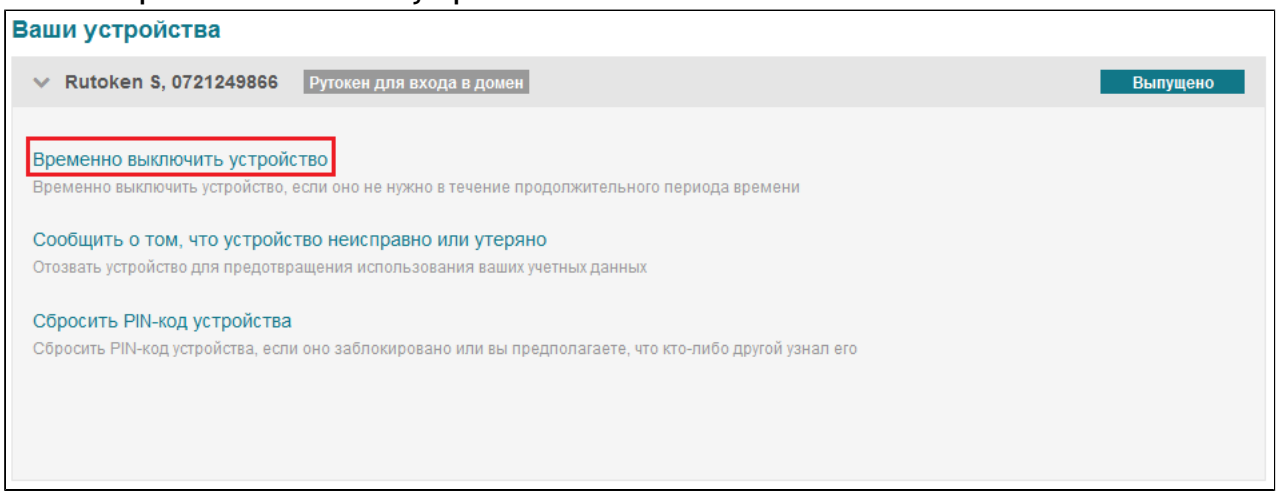
Важная информация

В зависимости от настроек системы могут быть доступны следующие действия:

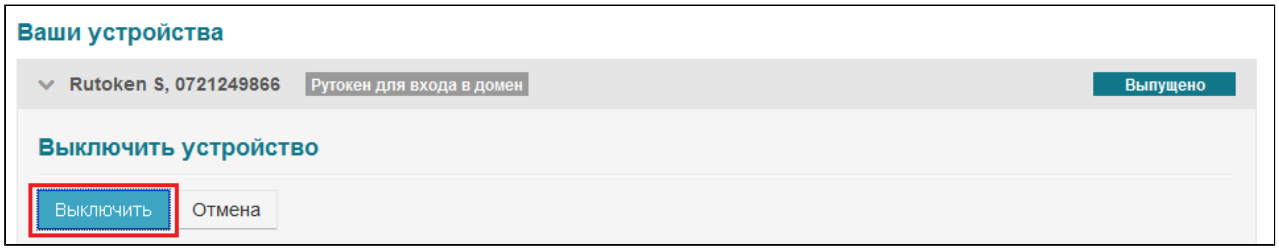
- Выключение и включение устройства
- Только выключение устройства
- Только включение устройства

Для выключения устройства выполните следующие действия:

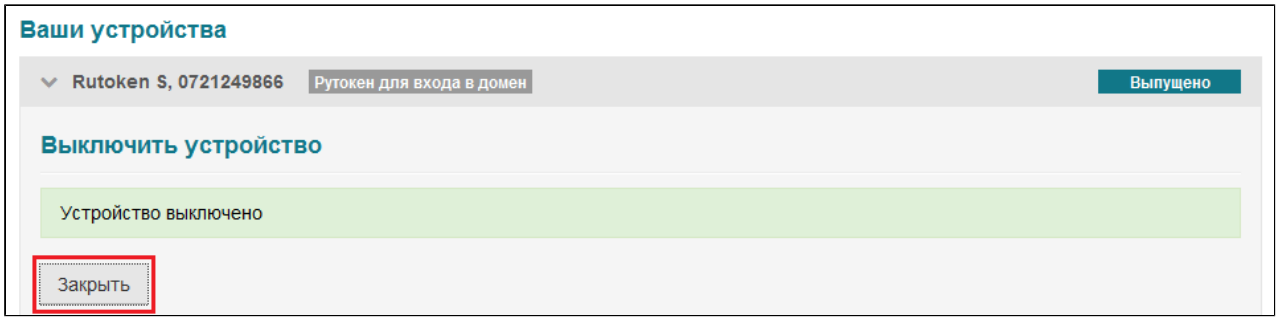
1. Нажмите **Временно выключить устройство**:



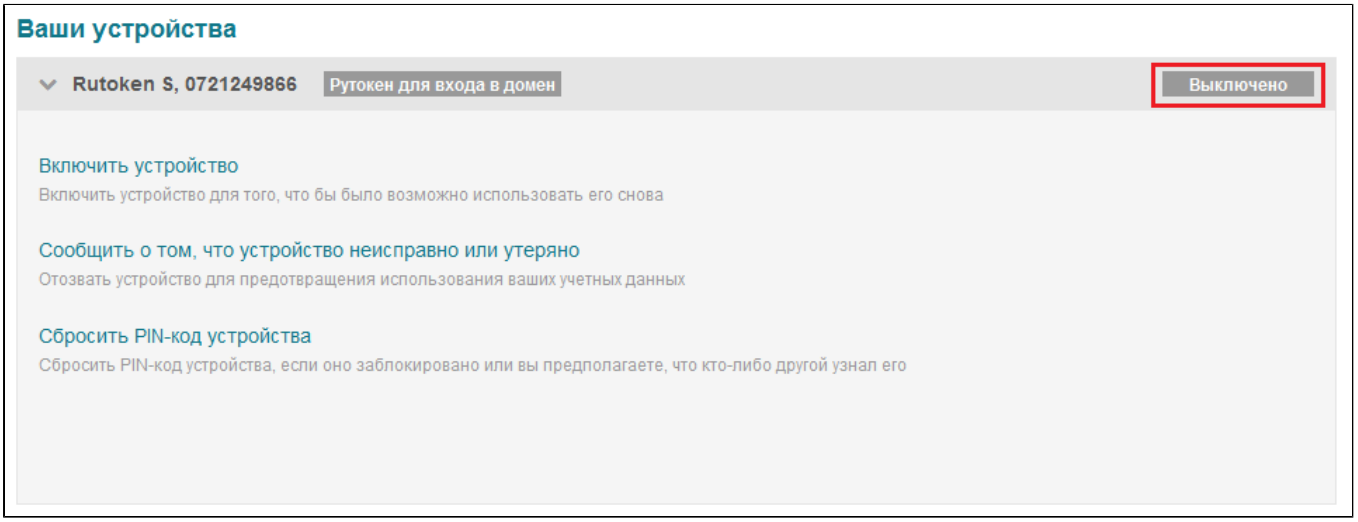
Подтвердите своё действие нажатием на кнопку **Выключить**:



После того как устройство будет выключено, нажмите **Закрыть**:



Статус устройства изменится с “Выпущено” на “Выключено”:

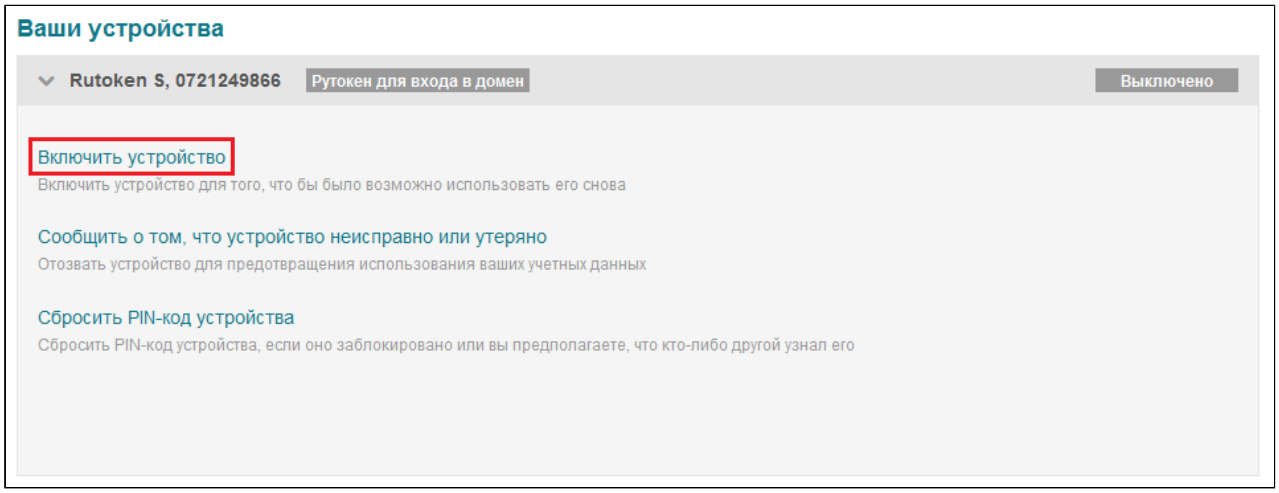


При попытке использования выключенного устройства для аутентификации будет получено сообщение о том, что все сертификаты отозваны.

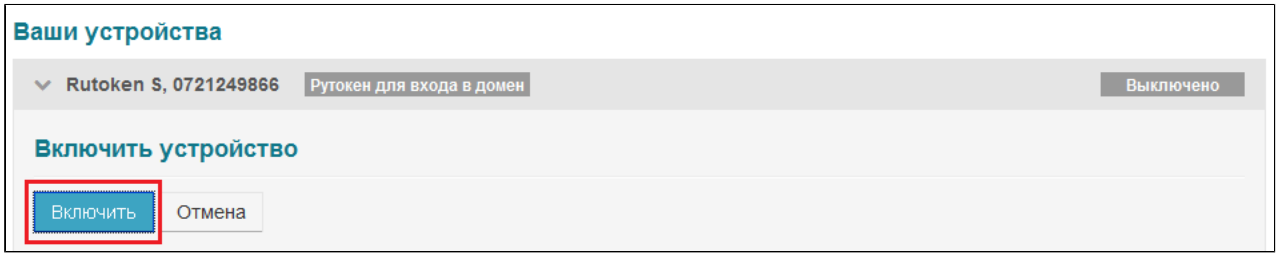
Включение устройства

Для включения устройства выполните следующие действия:

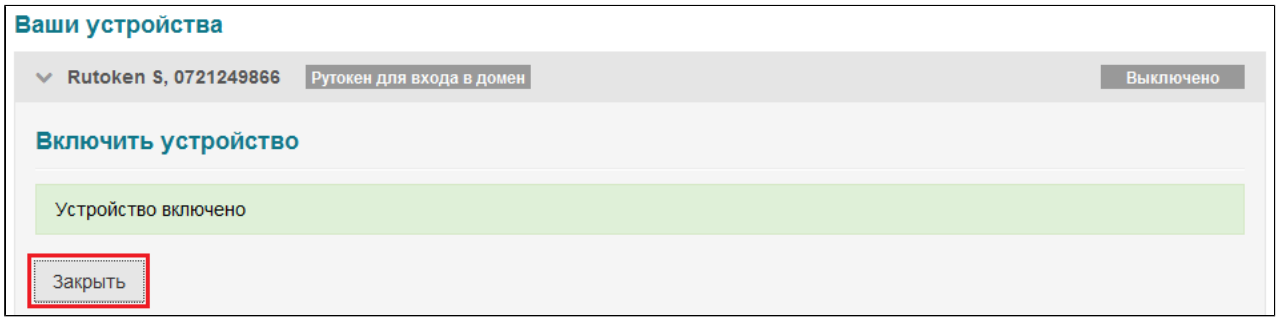
1. Нажмите **Включить устройство:**



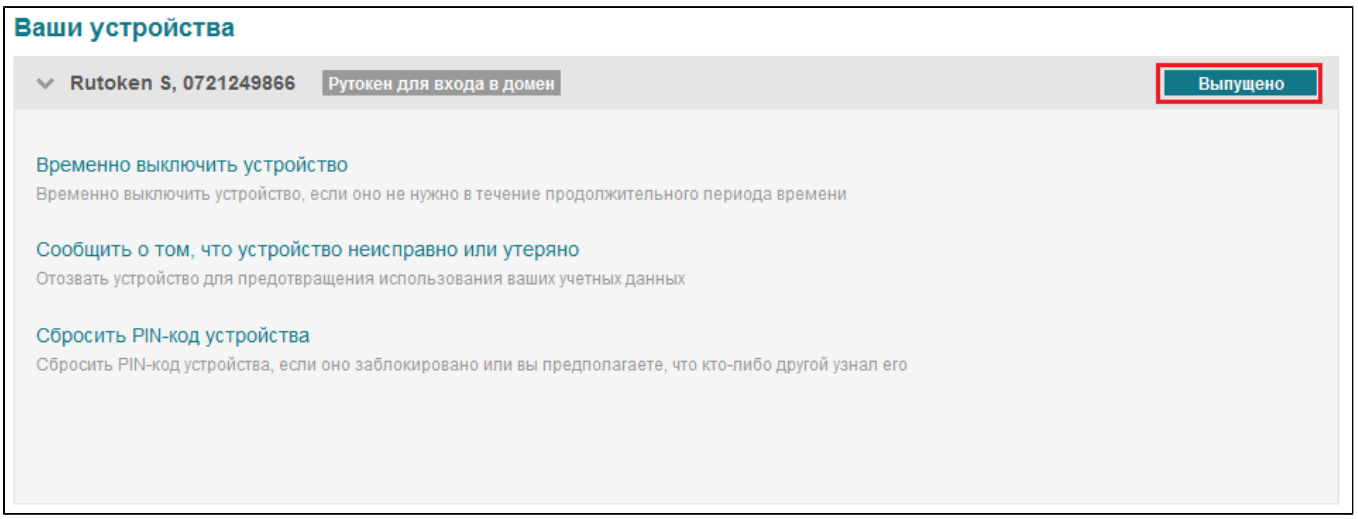
2. Подтвердите своё действие нажатием на кнопку **Включить:**



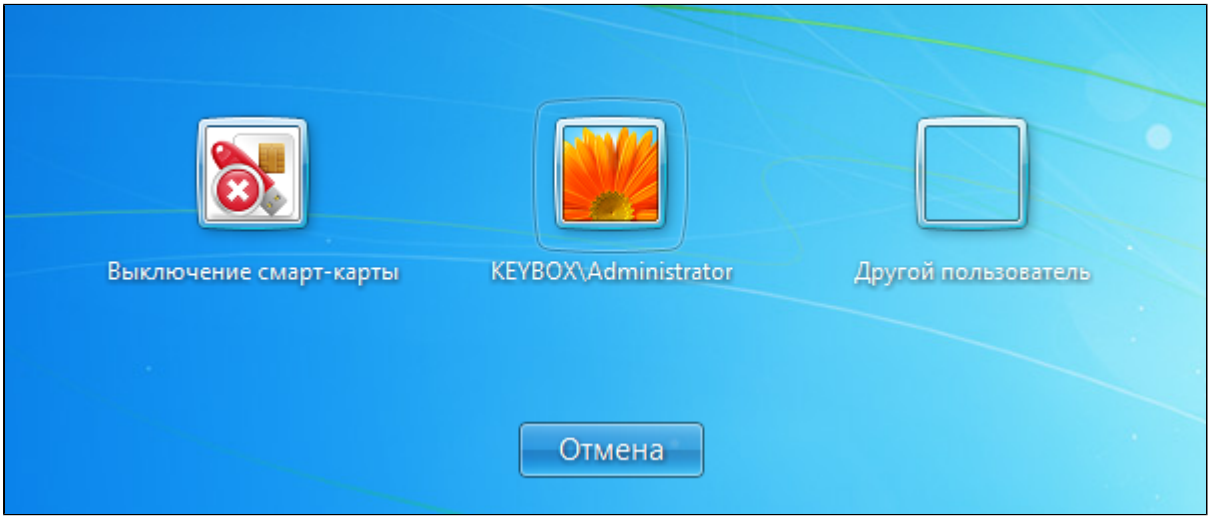
3. После того как устройство будет включено, нажмите **Закрыть**:



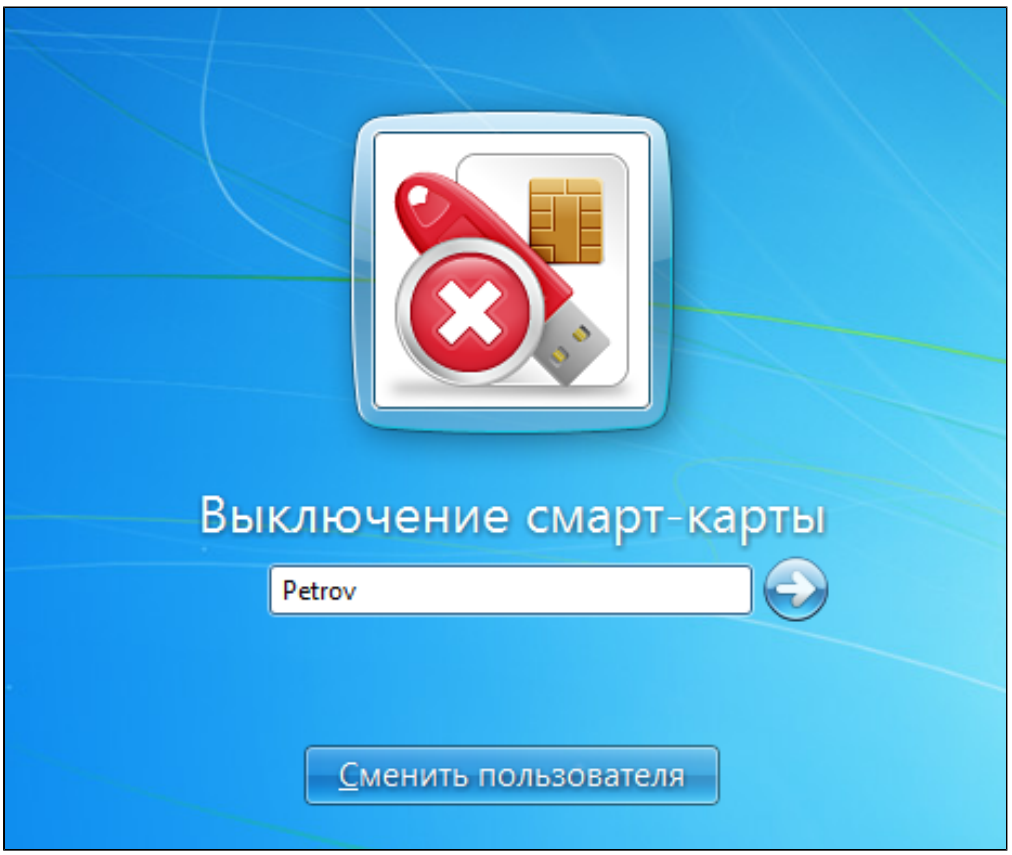
Статус устройства изменится с “Выключено” на “Выпущено”:



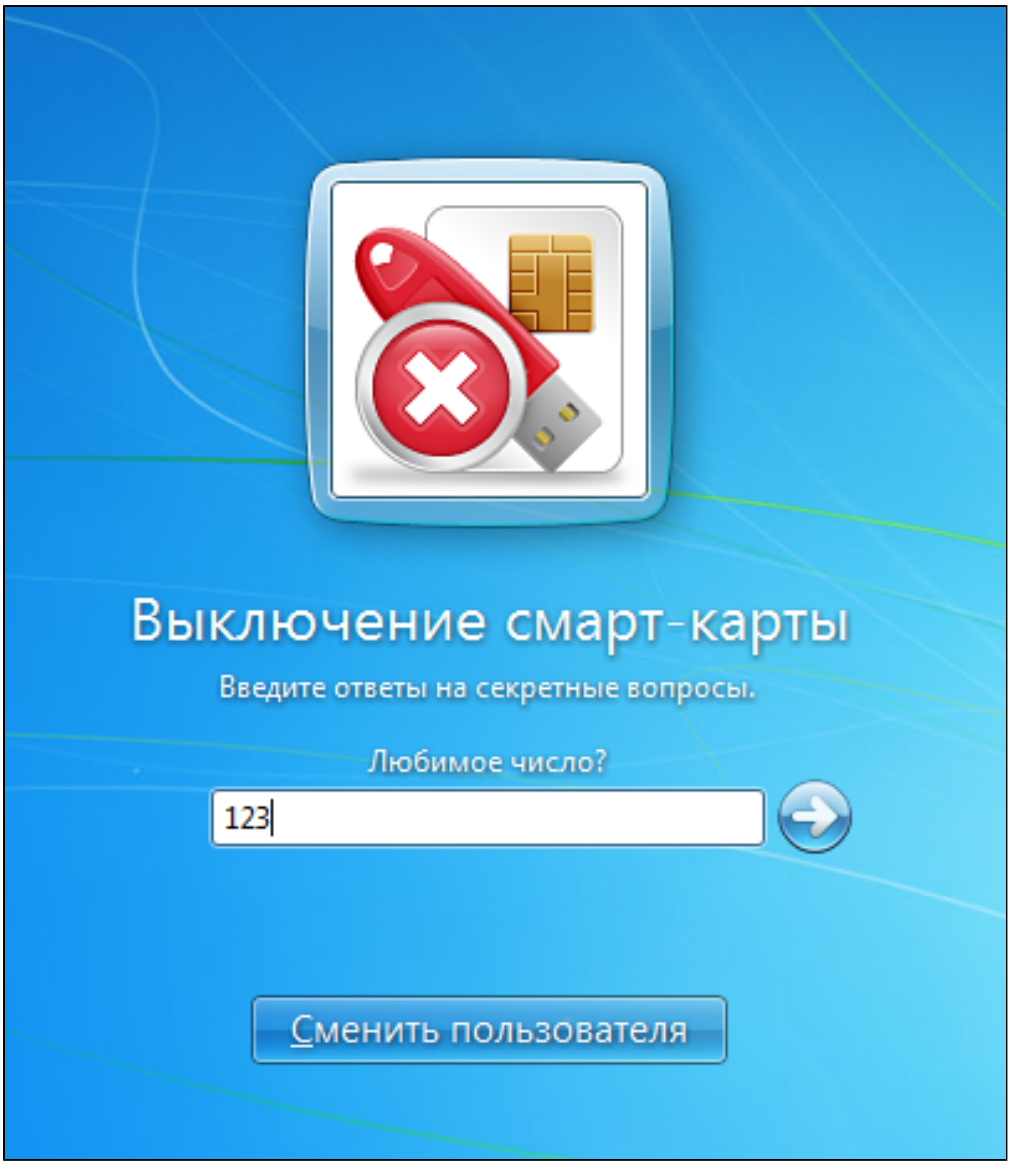
Выключить устройство так же можно из интерфейса входа, для этого нажмите **Выключение смарт-карты**:



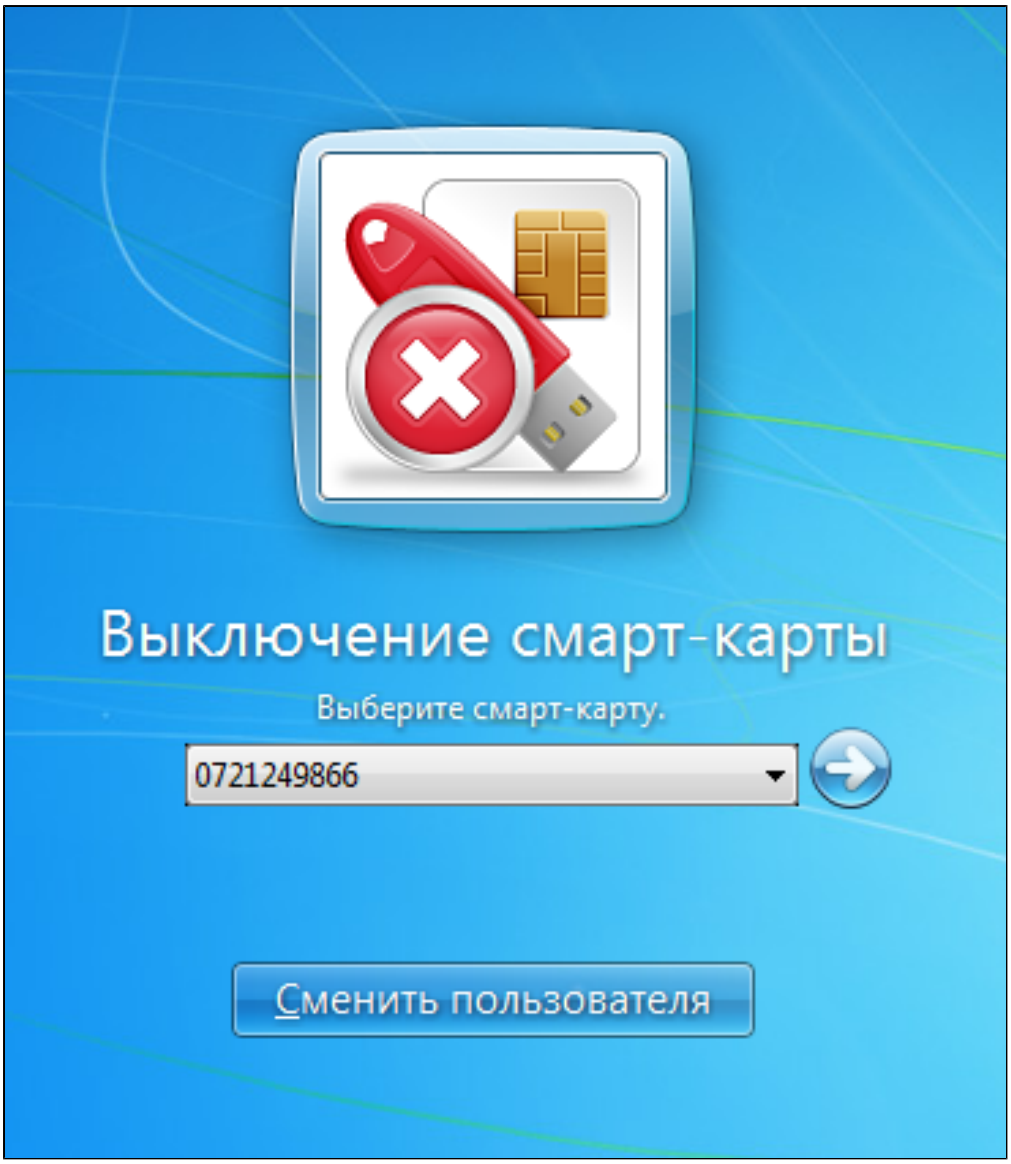
Введите имя пользователя и нажмите на  :



Введите ответ на секретный вопрос и нажмите на  :



Выберите операцию Выключить устройство и нажмите на  :



Устройство будет временно выключено. Включить его можно в личном кабинете или обратившись к сотруднику технической поддержки.

Отзыв устройства

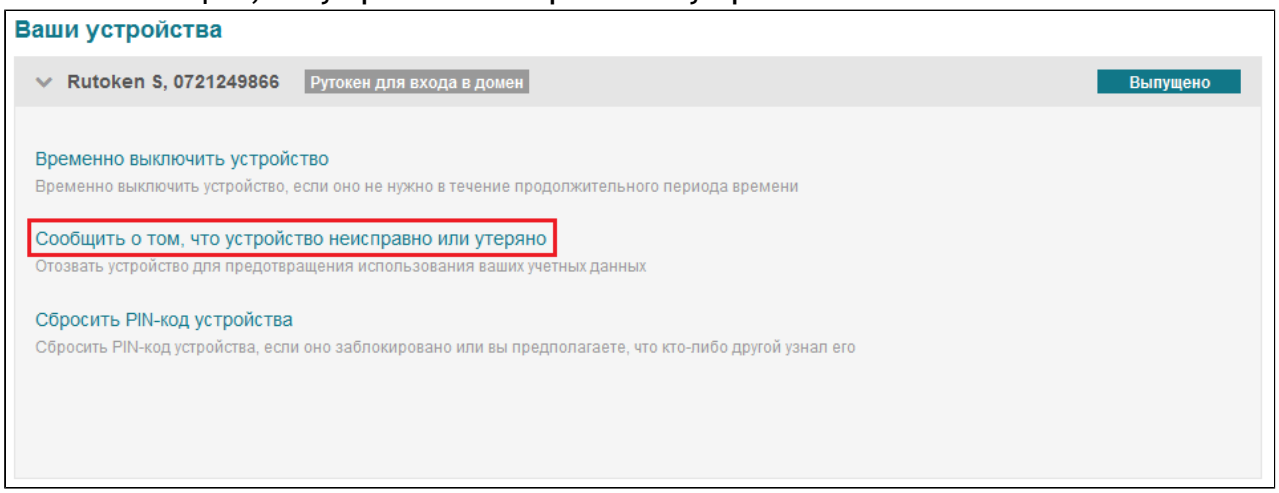
Устройство может быть отозвано в случае его повреждения или утери.

Важная информация

При отзыве устройства все сертификаты, хранящиеся на нем, будут отозваны без возможности их восстановления.

Для отзыва устройства выполните следующие действия:

1. Нажмите **Сообщить, что устройство неисправно или утеряно**:

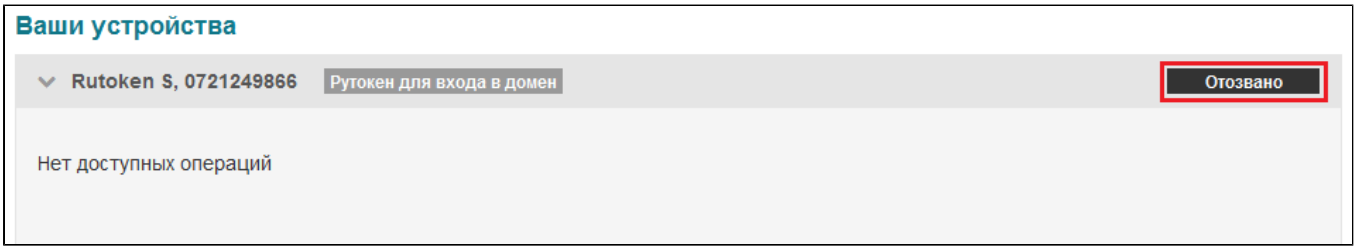


2. Укажите причину отзыва:

3. Нажмите кнопку **Отозвать**:

4. После того, как устройство будет отозвано, нажмите **Закрыть:**

Статус устройства изменится с “Выпущено” на “Отозвано”:



При попытке использования отозванного устройства для аутентификации будет выдано сообщение о том, что сертификаты отозваны.

Сброс и изменение PIN-кода

Если PIN-код устройства был забыт и устройство заблокировано, система позволяет сбросить PIN-код и задать новый. При этом устройство будет разблокировано.

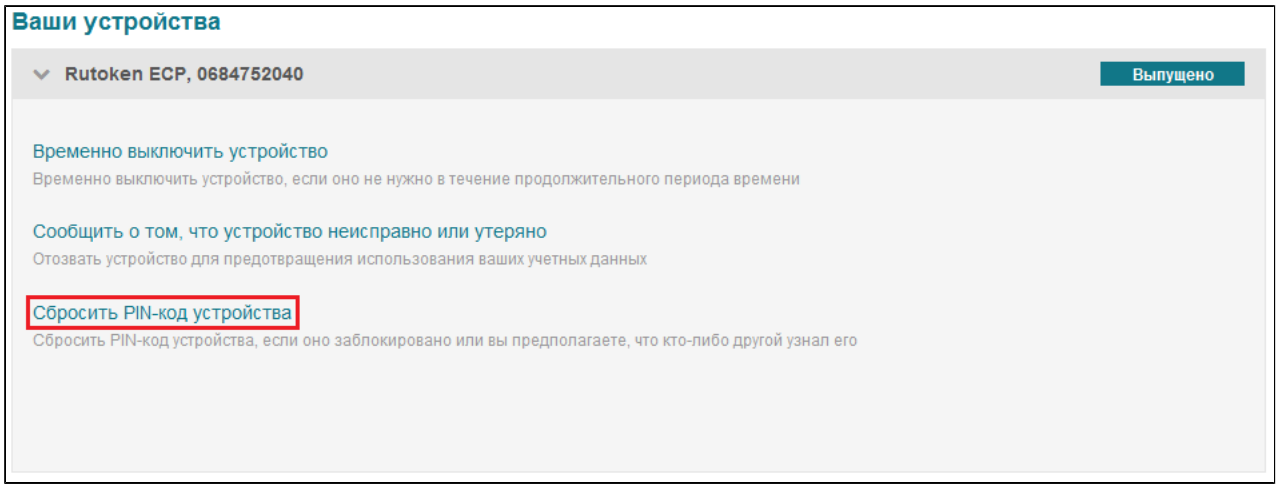
Важная информация

Возможность сброса PIN-кода настраивается администратором системы в политиках использования устройств. В зависимости от настроек может быть разрешен только сброс или только изменение PIN-кода.

Сброс PIN-кода

Для сброса PIN-кода устройства выполните следующие действия:

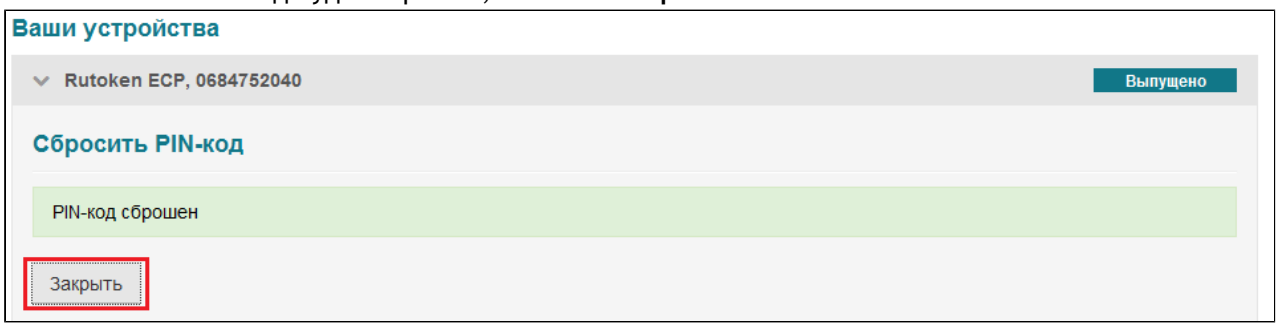
1. Подключите устройство к компьютеру и нажмите **Сбросить PIN-код устройства**:



2. Задайте новый PIN-код и подтвердите его:

3. Нажмите **Сбросить**:

4. После того как PIN-код будет сброшен, нажмите **Закрыть:**

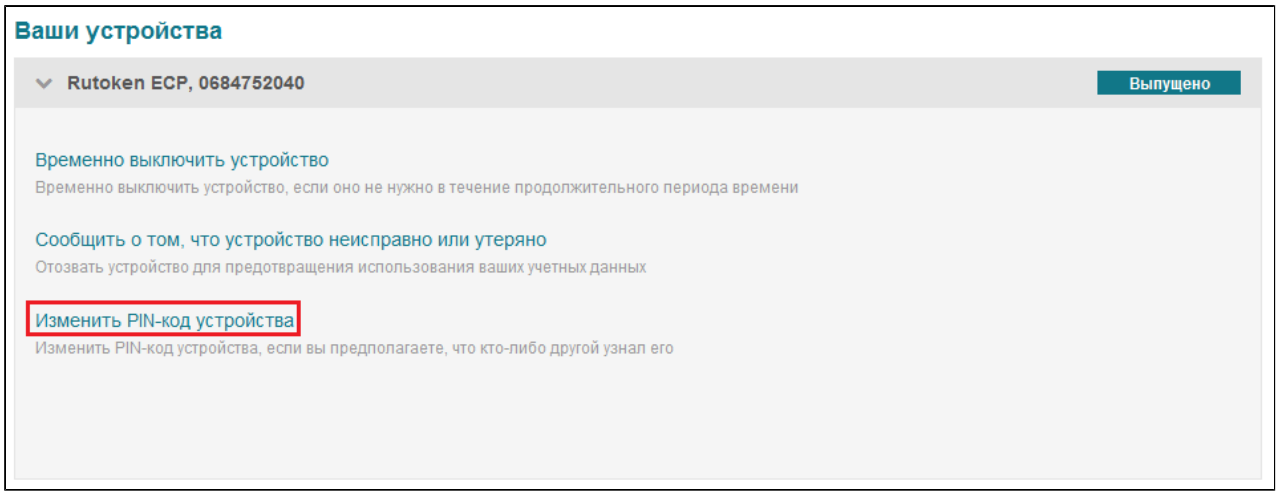


Изменение PIN-кода

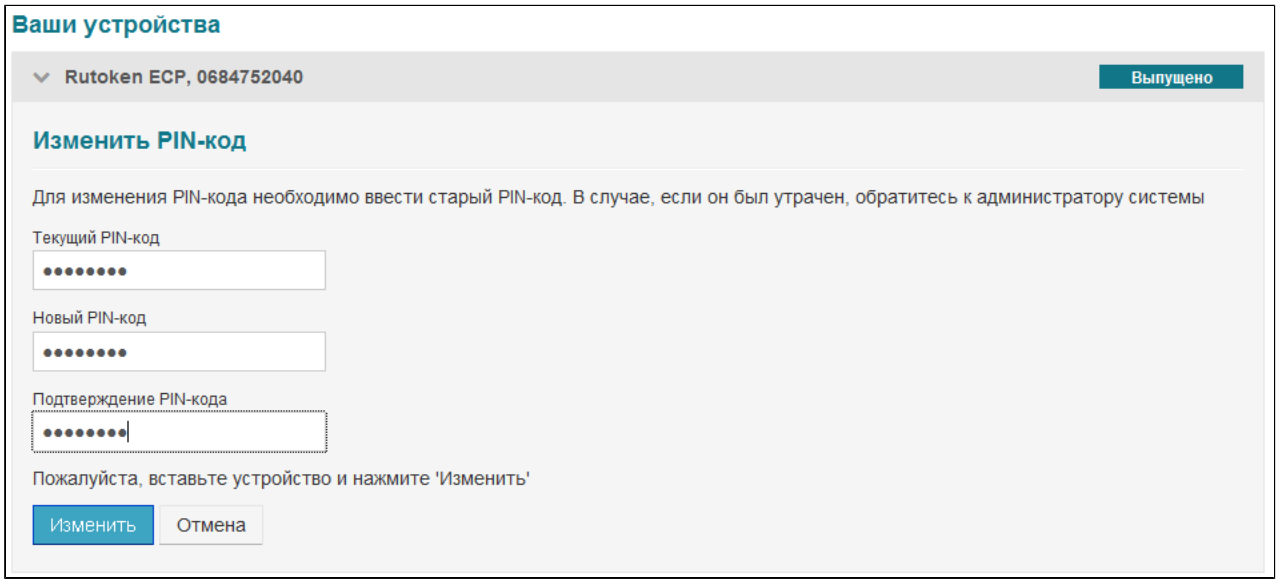
Если есть основания полагать, что PIN-код устройства стал известен кому-то другому, то он может быть изменен.

Для изменения PIN-кода устройства выполните следующие действия:

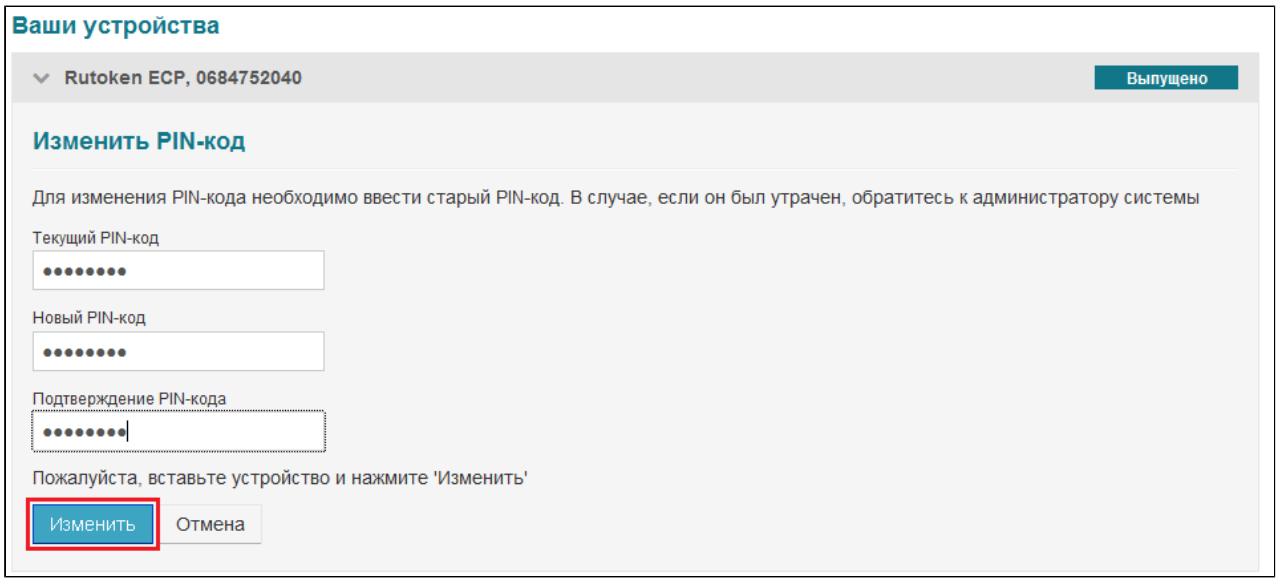
1. Подключите устройство к компьютеру и н ажмите **Изменить PIN-код устройства**:



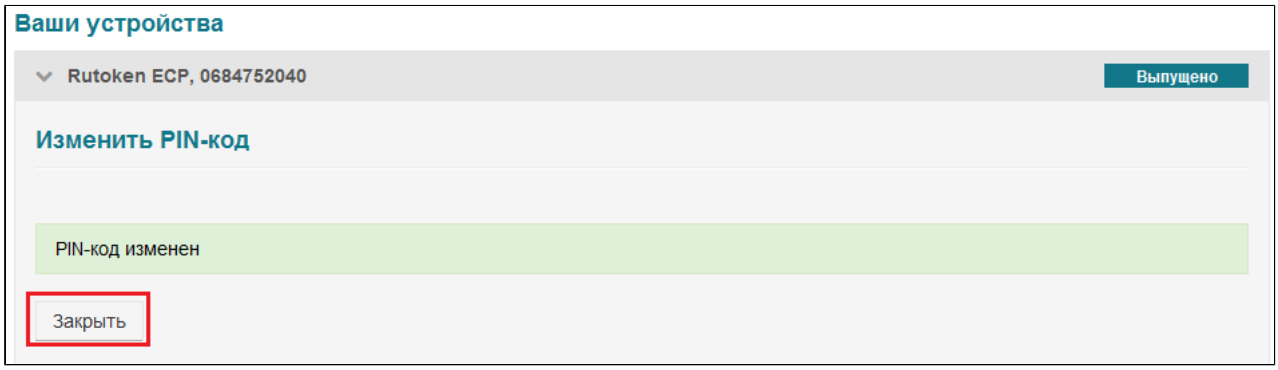
2. Введите текущий PIN-код, задайте новый PIN-код и подтвердите его:



3. Нажмите **Изменить**:

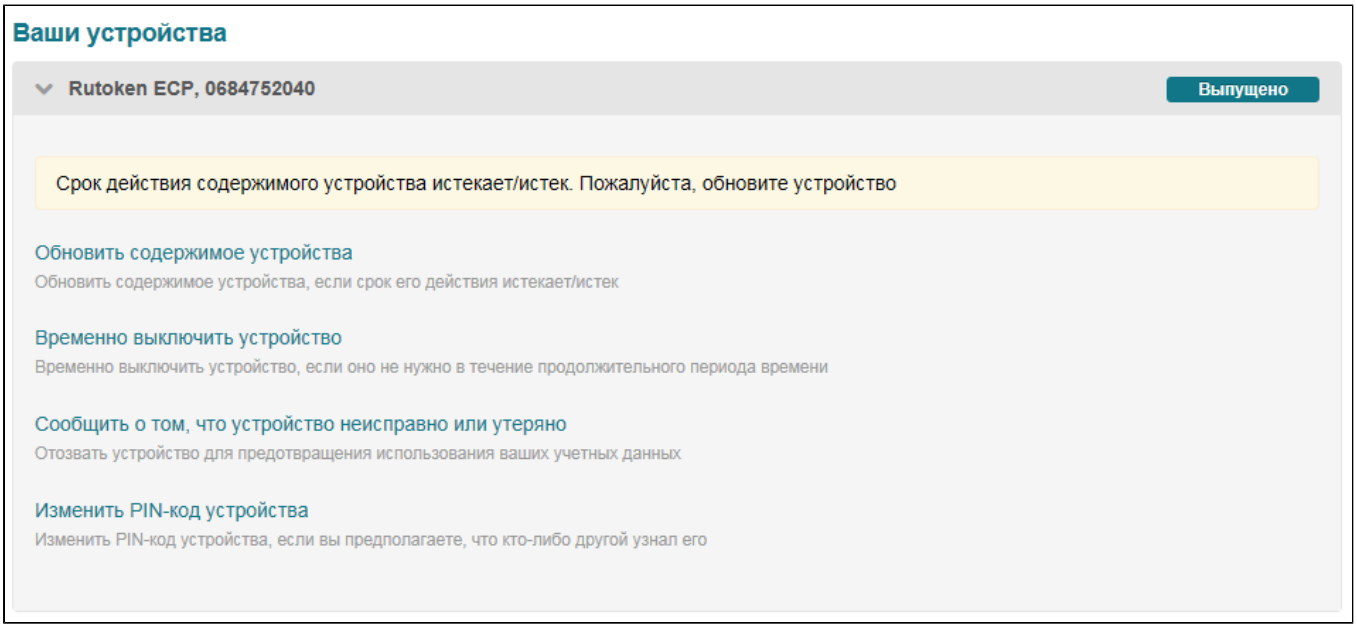


4. После того как PIN-код будет изменен, нажмите **Закрыть**:



Обновление устройства

Если срок действия одного или нескольких сертификатов, находящихся на устройстве, истек, система позволяет обновить их, так же обновление доступно, если в политику были добавлены новые шаблоны сертификатов. В случае если срок действия сертификата истек, в личном кабинете будет отображено соответствующее сообщение:

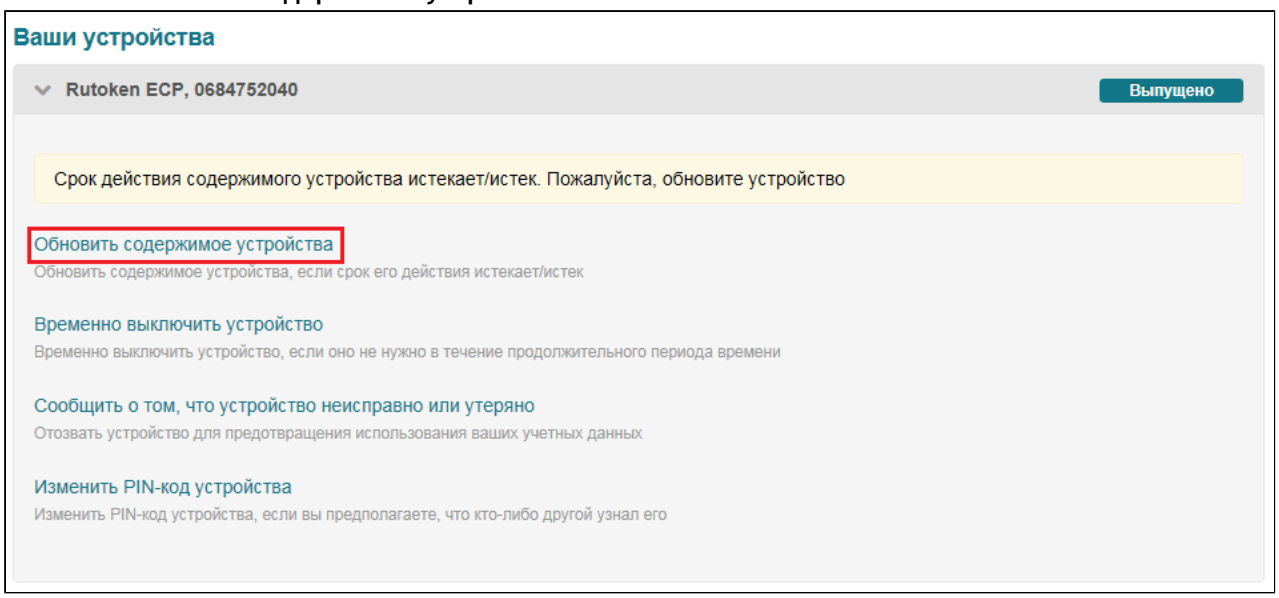


Важная информация

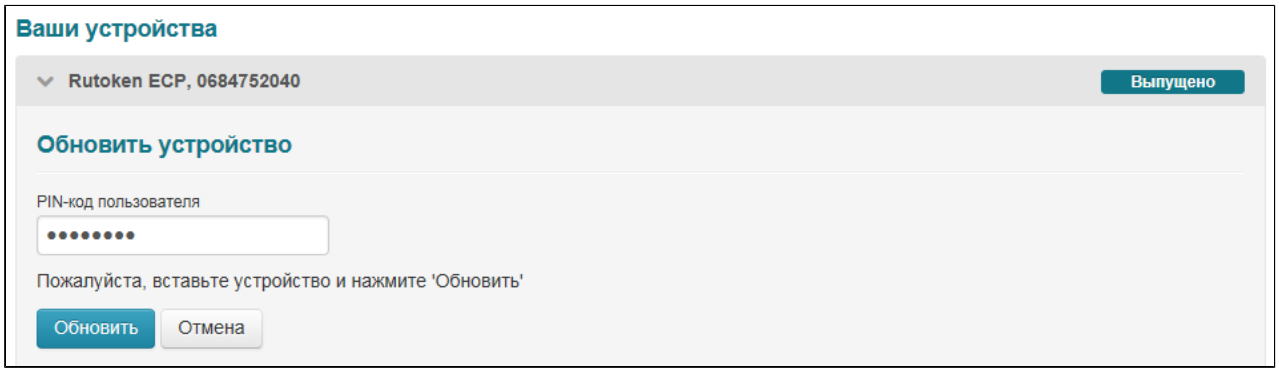
Возможность обновления устройства настраивается администратором системы в политиках использования устройств.

Для обновления устройства выполните следующие действия:

1. Нажмите **Обновить содержимое устройства**:



2. Подключите устройство к компьютеру, введите PIN-код и нажмите **Обновить**:

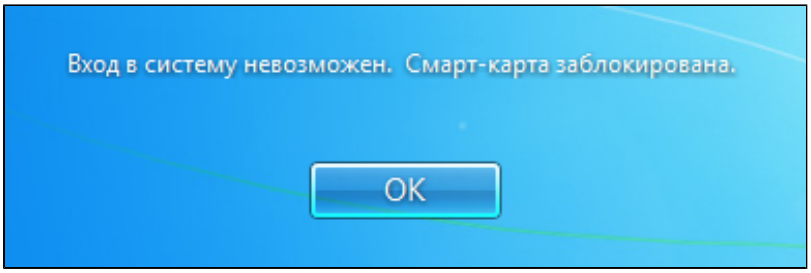


3. После того как устройство будет обновлено, нажмите **Закрыть.**

Разблокировка устройства

Если PIN-код устройства был введен неверно несколько раз подряд, то оно блокируется. Максимальное количество попыток ввода PIN-кода пользователем устройства и может быть различным для разных устройств .

Если устройство было заблокировано при попытке входа в систему, то будет выдано соответствующее сообщение:



Для разблокировки устройства нажмите на кнопку ОК.

В случае если имеется подключение к серверу Рутокен KeyBox, будет доступна онлайн разблокировка. Онлайн-разблокировка не требует взаимодействия с сотрудником технической поддержки.

Для онлайн-разблокировки:

1. Введите ответы на секретные вопросы:
2. Введите новый PIN-код пользователя и его подтверждение, нажмите на кнопку:

Устройство будет разблокировано:

В случае если соединение с сервером отсутствует, производится офлайн-разблокировка.

При офлайн-разблокировке необходимо связаться с сотрудником технической поддержки.

1. В случае офлайн-разблокировки системой будет сгенерирован запрос, который необходимо передать сотруднику технической поддержки.
2. Для подтверждения личности владельца устройства сотрудник технической поддержки запросит ответы на секретные вопросы. В случае верных ответов пользователю предоставляется код для разблокировки. Введите его в поле **Ответ**:
3. Введите новый PIN-код, его подтверждение и нажмите на соответствующую кнопку.

Устройство будет разблокировано.

Важная информация

Изменить секретные вопросы и ответы на них можно в Self Service.

Выполните вход в систему, используя новый PIN-код.

Если устройство не используется для входа в домен и было заблокировано в процессе работы, то для его разблокировки необходимо использовать утилиту Рутокен KeyBox Unblock.

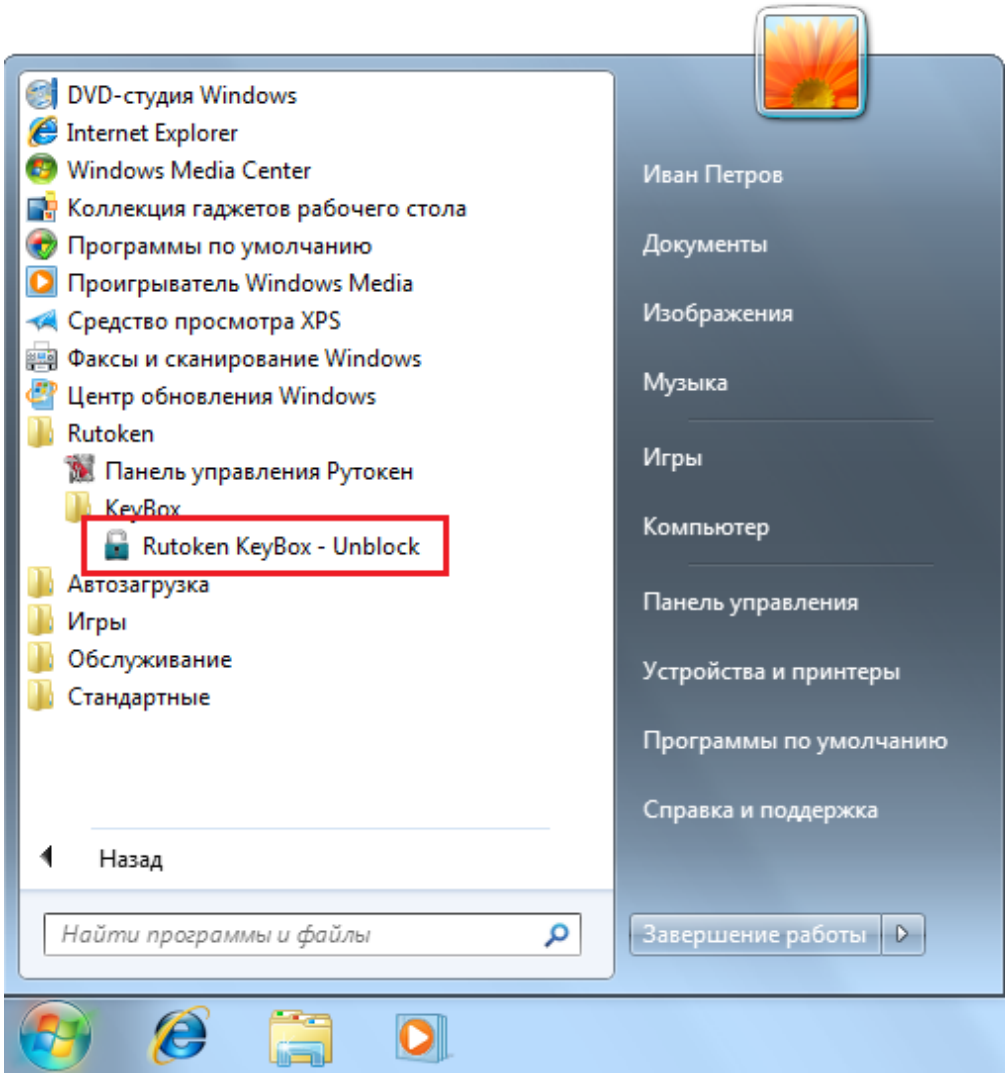
Утилита входит в состав дистрибутива RutokenKeyBoxClientTools.

Важная информация

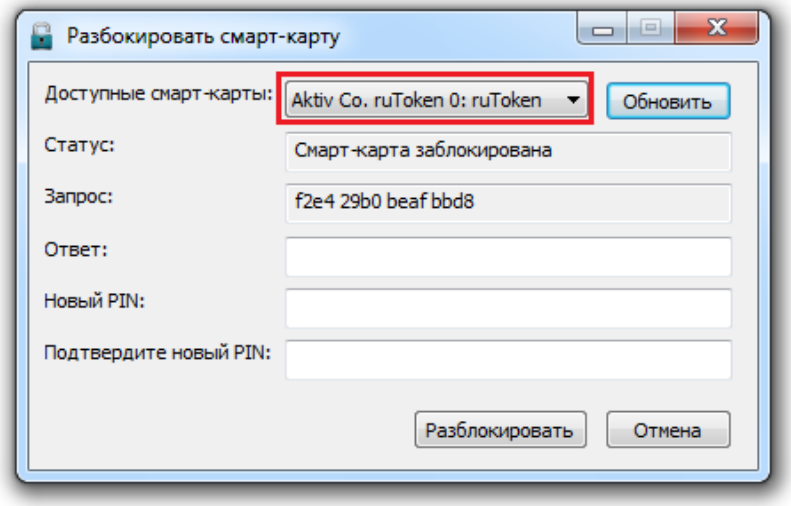
Офлайн-разблокировка может быть запрещена политик администратором.

Для разблокировки устройства:

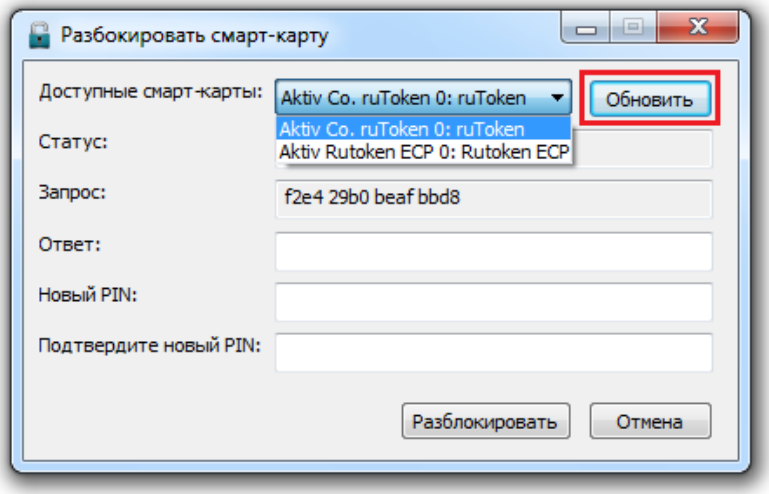
1. Запустите утилиту разблокировки (**Пуск/ Программы/ Rutoken/ KeyBox/ Rutoken KeyBox - Unblock**):



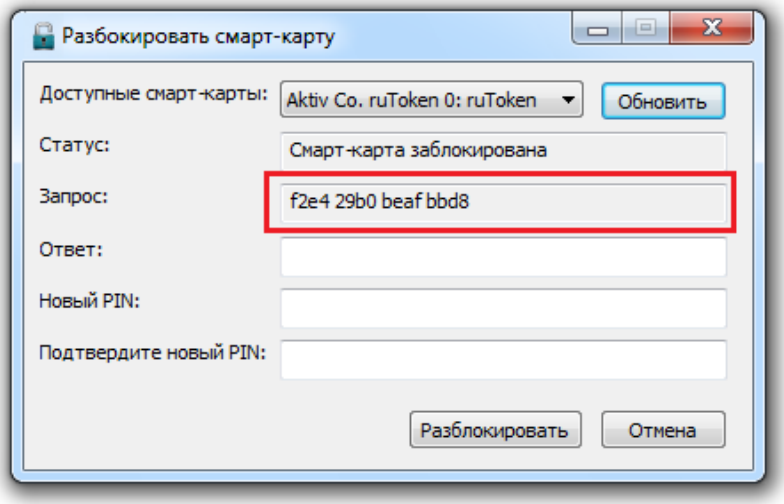
2. Подключите устройство. После подключения утилита обнаружит его автоматически:



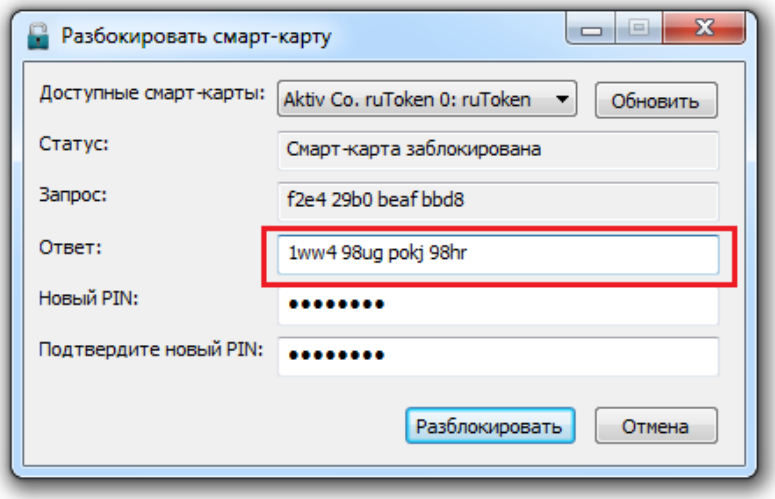
Если подключено несколько устройств, необходимо выбрать нужное устройство из выпадающего списка и нажать на кнопку **Обновить**:



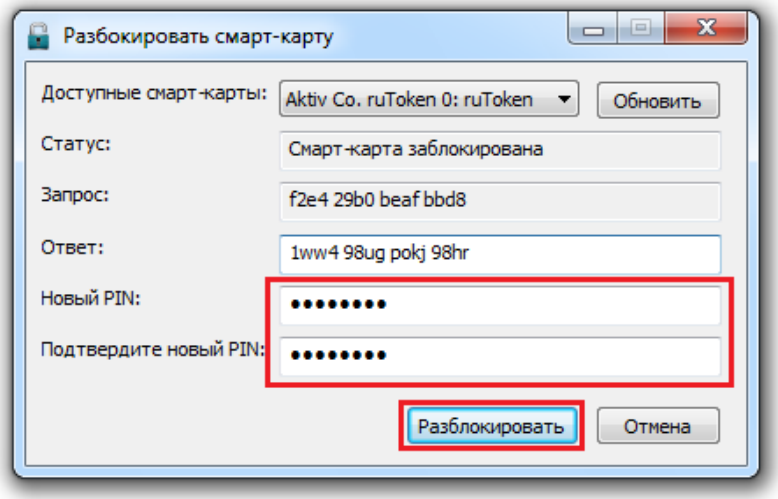
3. В поле **Запрос** будет автоматически сгенерирован запрос на разблокировку устройства. Свяжитесь с сотрудником технической поддержки и сообщите ему запрос.



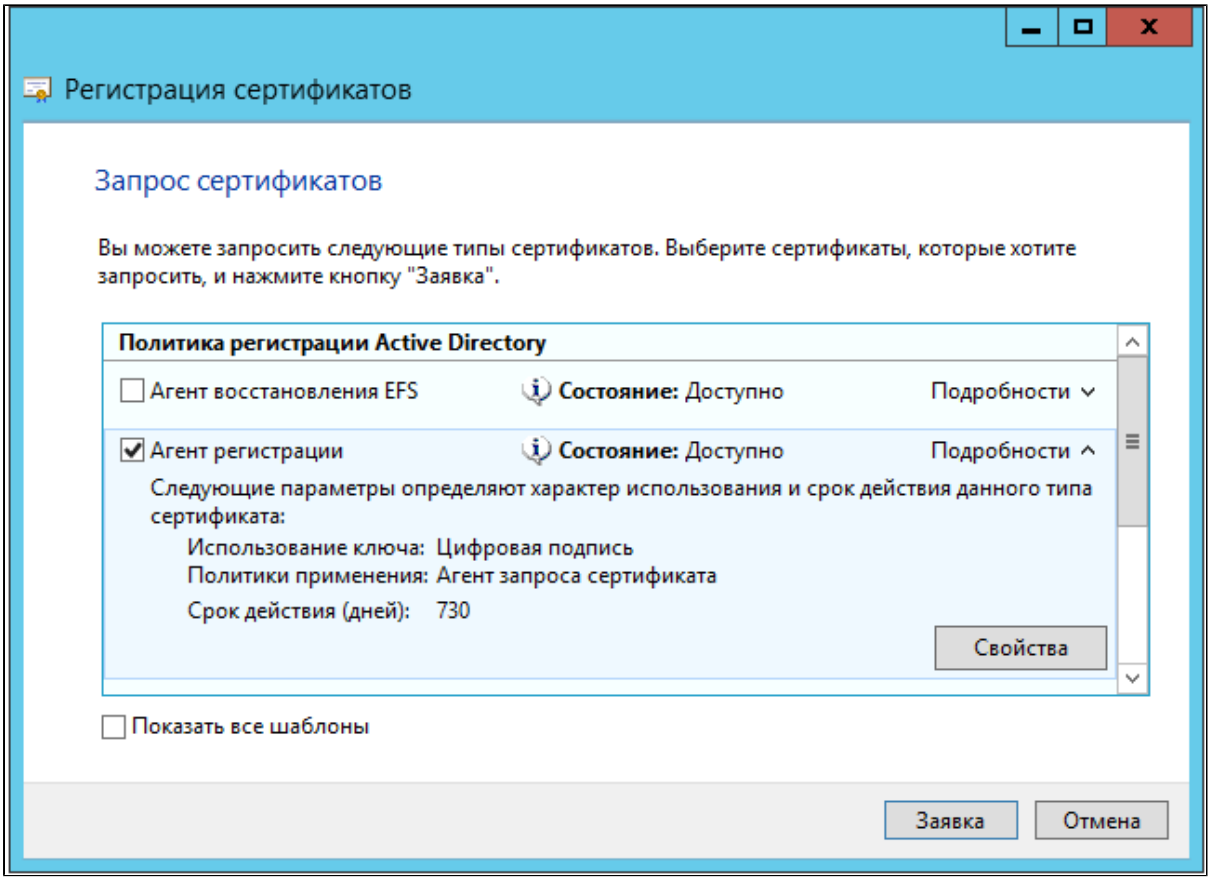
4. Сотрудник технической поддержки запросит ответы на секретные вопросы для подтверждения личности владельца устройства. В случае корректных ответов сотрудник технической поддержки сообщит код, необходимый для завершения разблокировки устройства. Введите полученный код в поле Ответ утилиты разблокировки:



5. Введите новый PIN-код, его подтверждение и нажмите на кнопку Разблокировать:



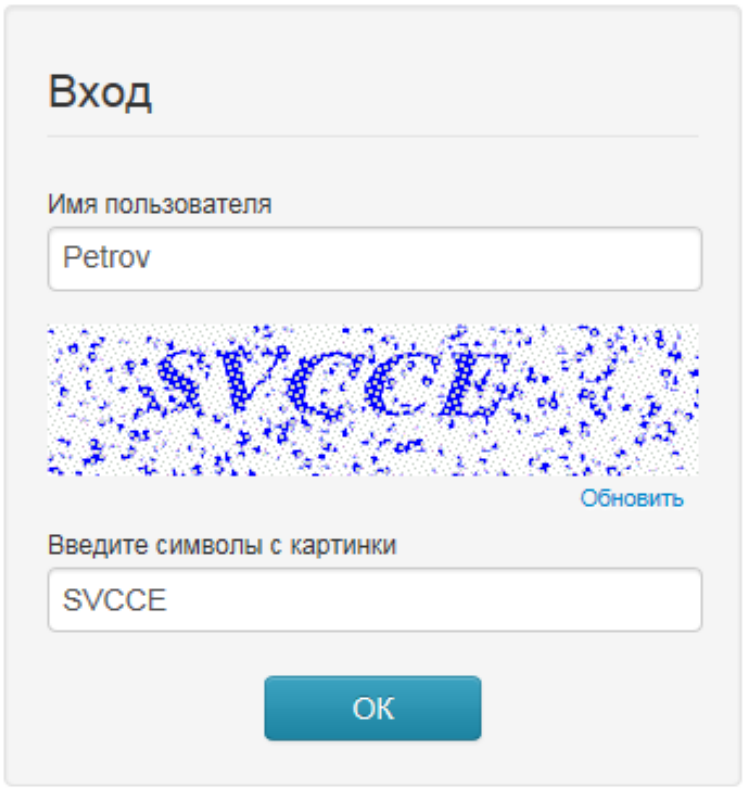
Устройство будет разблокировано, PIN-код изменен. Значение в поле Статус утилиты изменится на "Смарт-карта не заблокирована":



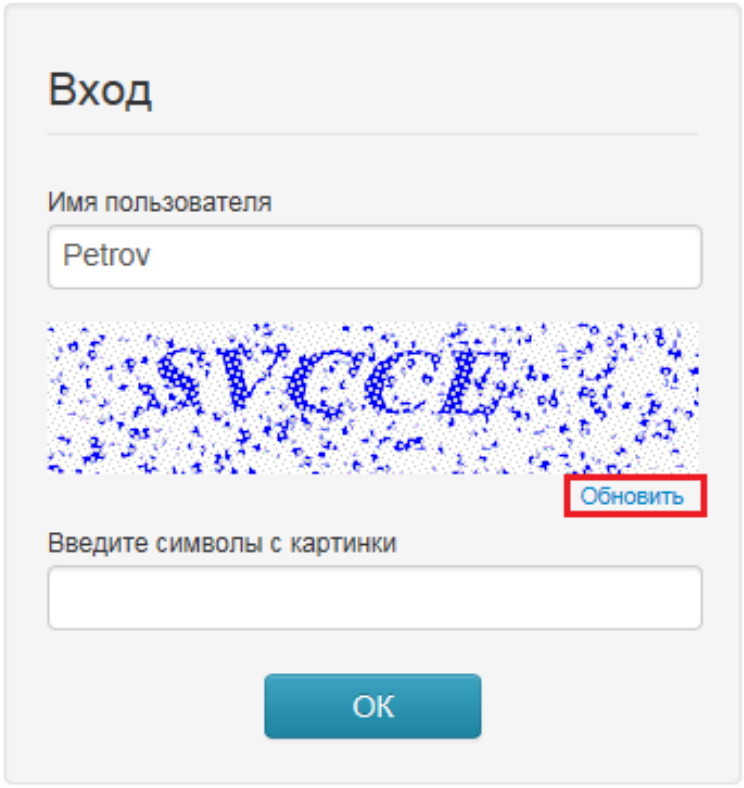
Удаленный личный кабинет

Для доступа к управлению устройствами за пределами корпоративного домена в системе реализован удаленный личный кабинет пользователя - Remote Self Service. Приложение Remote Self Service предназначено для выполнения ограниченного набора операций с устройством с любого компьютера, подключенного к сети Интернет (из командировки, из дома и т.п.). Доступ к приложению осуществляется по адресу **https://<адрес сервераРутокен KeyBox>/ keyboxremote/**

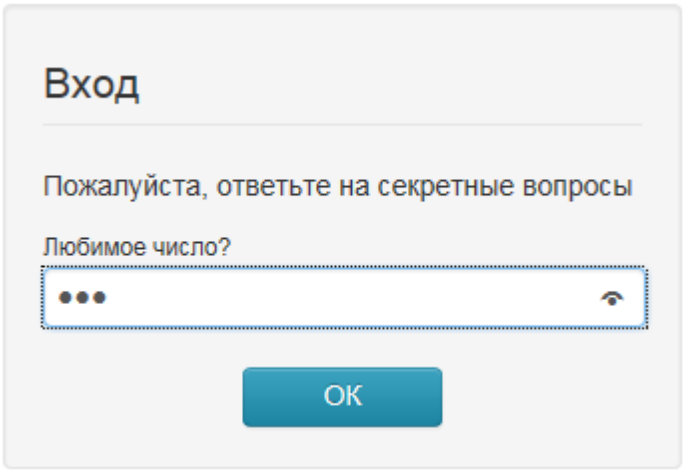
Для использования Remote Self Service необходимо перейти по соответствующему адресу, ввести своё имя и символы с изображения:



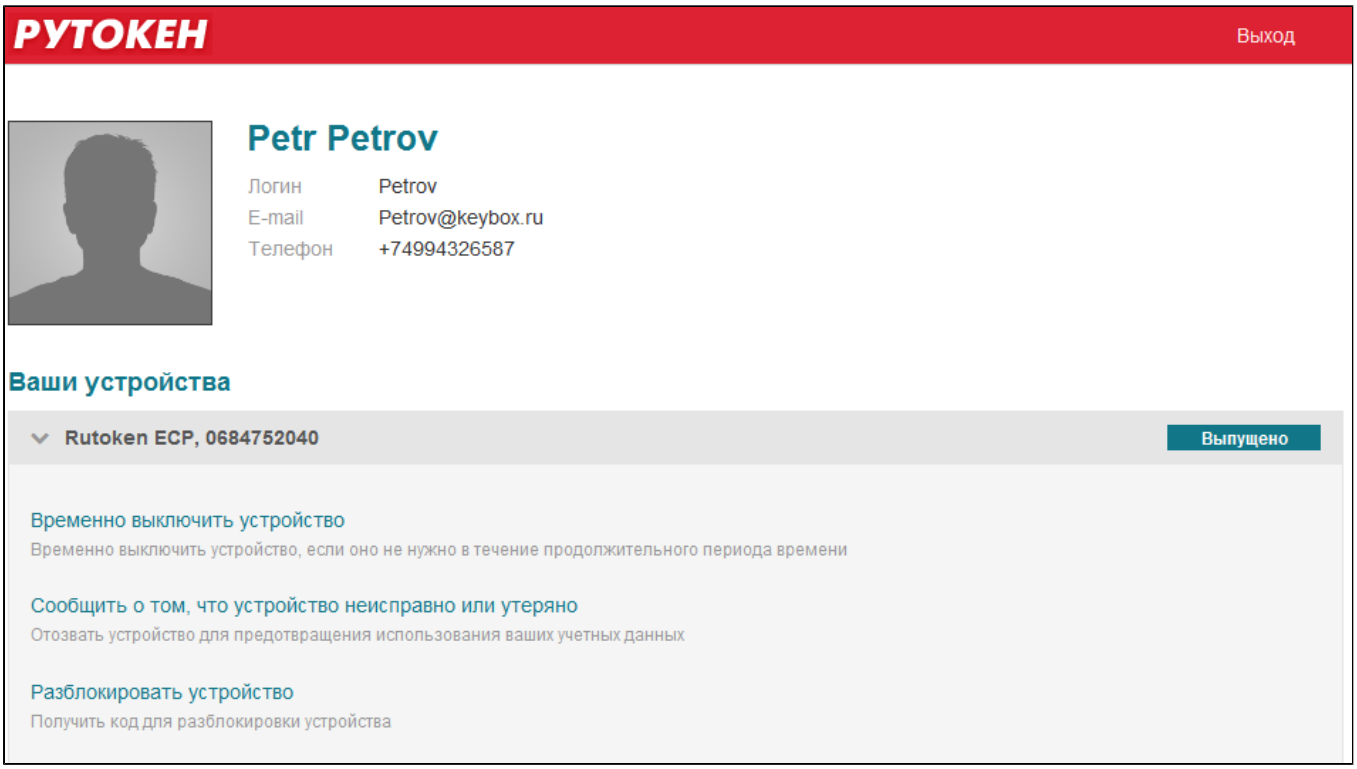
Если символы плохо различимы, то можно обновить изображение, нажав на ссылку **Обновить**:



После ввода логина необходимо пройти аутентификацию по секретным вопросам:



В случае верных ответов на секретные доступ к Remote Self Service будет предоставлен:



Важная информация

Если Вы не можете войти в приложение, обратитесь к администратору.

Набор действий, доступных пользователю в приложении Self Service , определяется администратором системы. В данном руководстве описаны все возможные действия, доступные пользователю.

В приложении доступны следующие функции:

- Выключение устройства
- Включение устройства
- Отзыв устройства
- Разблокировка устройства

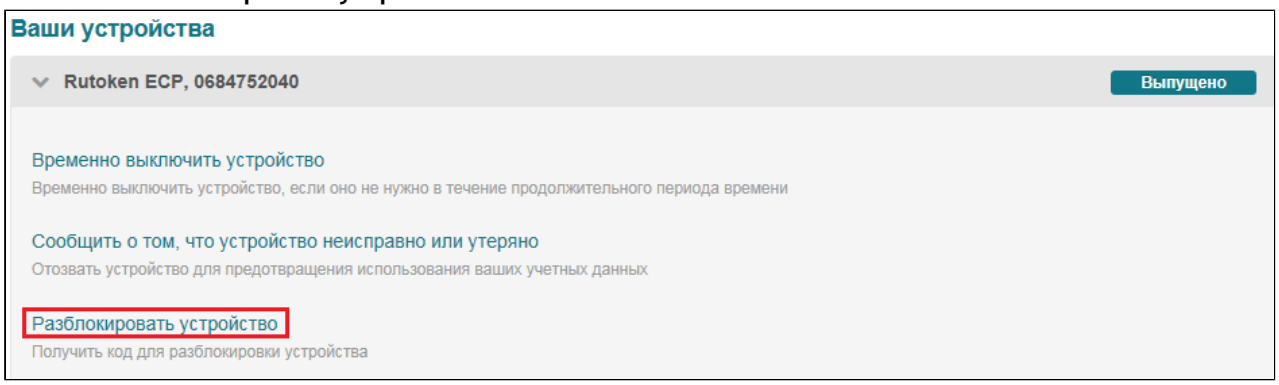
Операции выключения\включения устройства и отзыва производятся так же как и в личном кабинете пользователя.

Разблокировка устройства

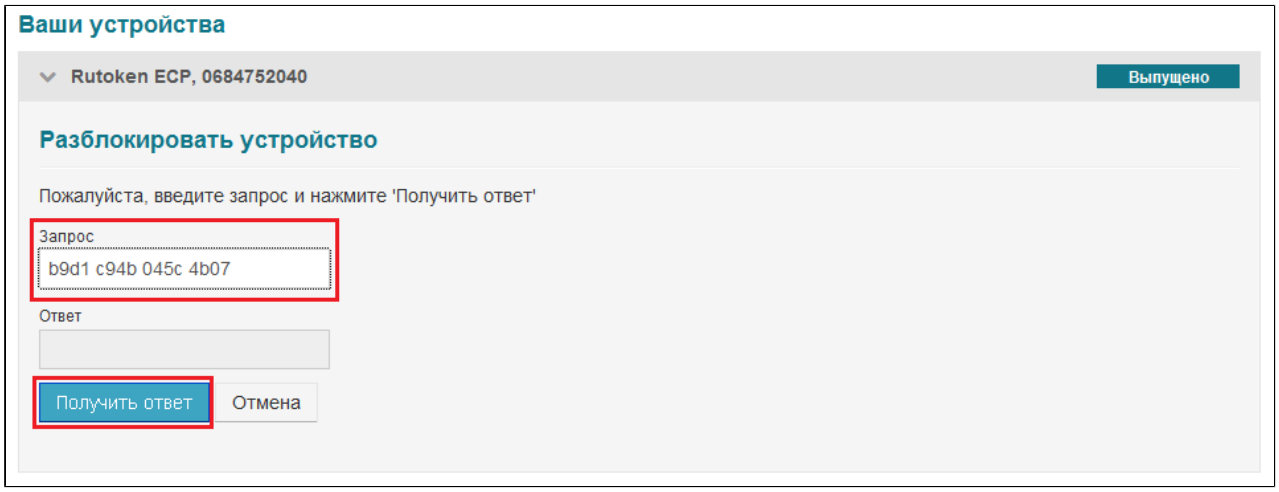
Если PIN-код устройства был забыт и устройство заблокировано система позволяет разблокировать его и сменить PIN-код.

Для разблокировки устройства:

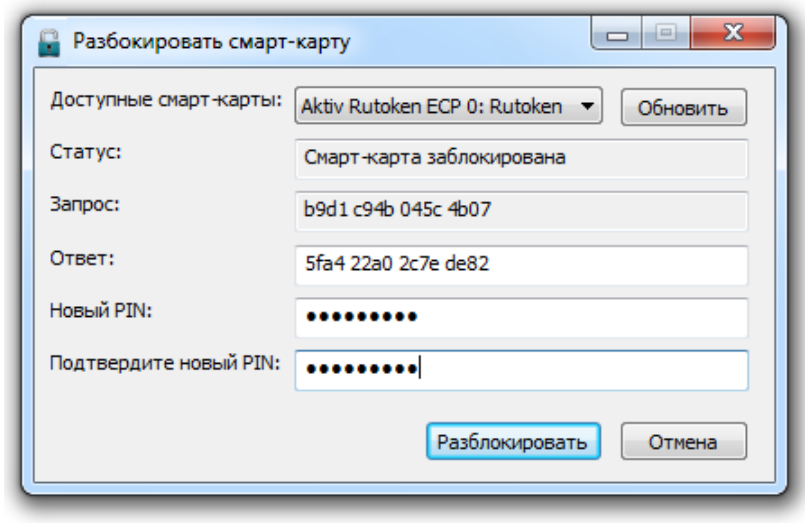
1. Нажмите **Разблокировать устройство**:



2. Сгенерируйте запрос используя утилиту разблокировки (см. пункт Разбловировка устройства), введите его в поле **Запрос** и нажмите на кнопку **Получить ответ**:

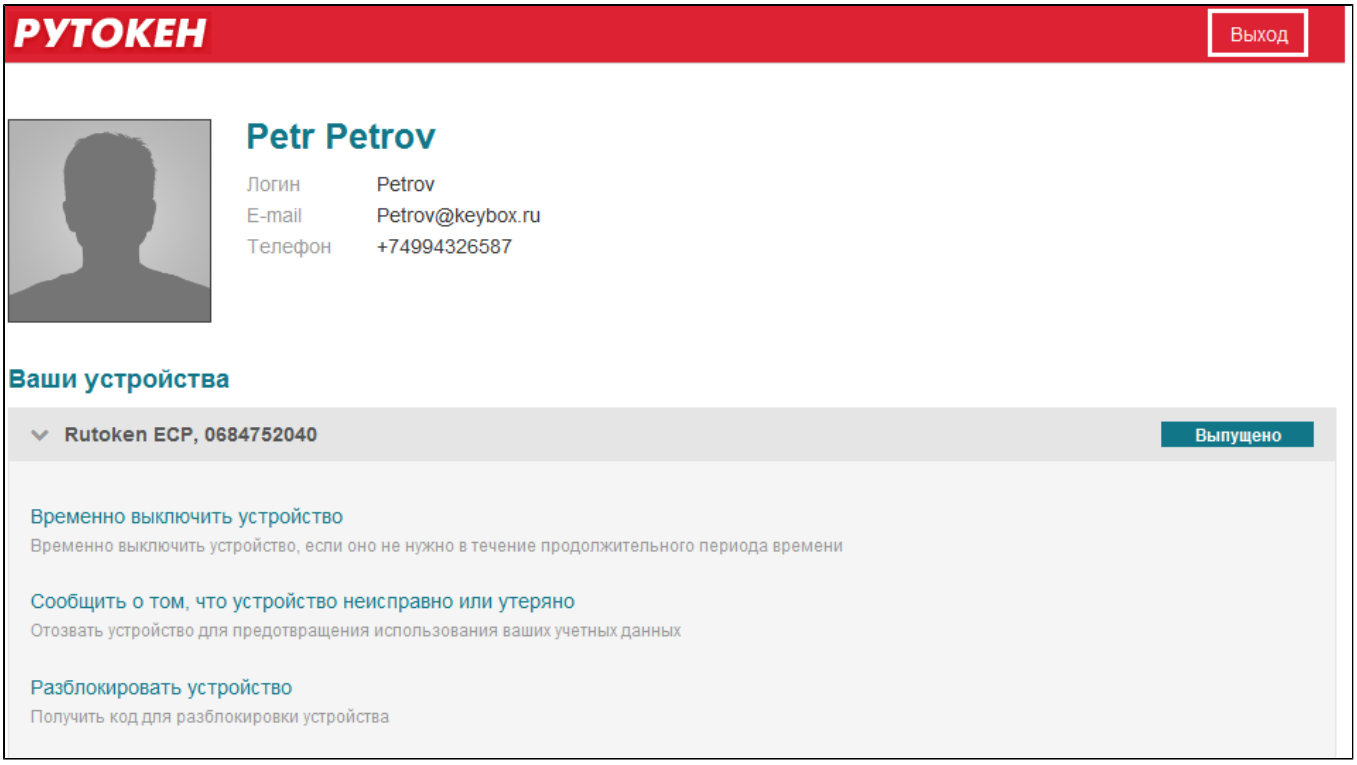


3. Введите полученный ответ в окно утилиты разблокировки, ведите новый PIN-код и его подтверждение и нажмите на кнопку Разблокировать:



Устройство будет разблокировано.

После завершения работы с удаленным личным кабинетом необходимо закончить сеанс работы, нажав на ссылку в правой верхней части окна **Выход**:



Раздел 5. Работа с утилитой разблокировки

Общая информация

Рутокен KeyBox Unblock - утилита, предназначенная для офлайн-разблокировки устройств в случае отсутствия подключения к серверу Рутокен KeyBox.

Утилита входит в состав дистрибутива RutokenKeyBoxClientTools.

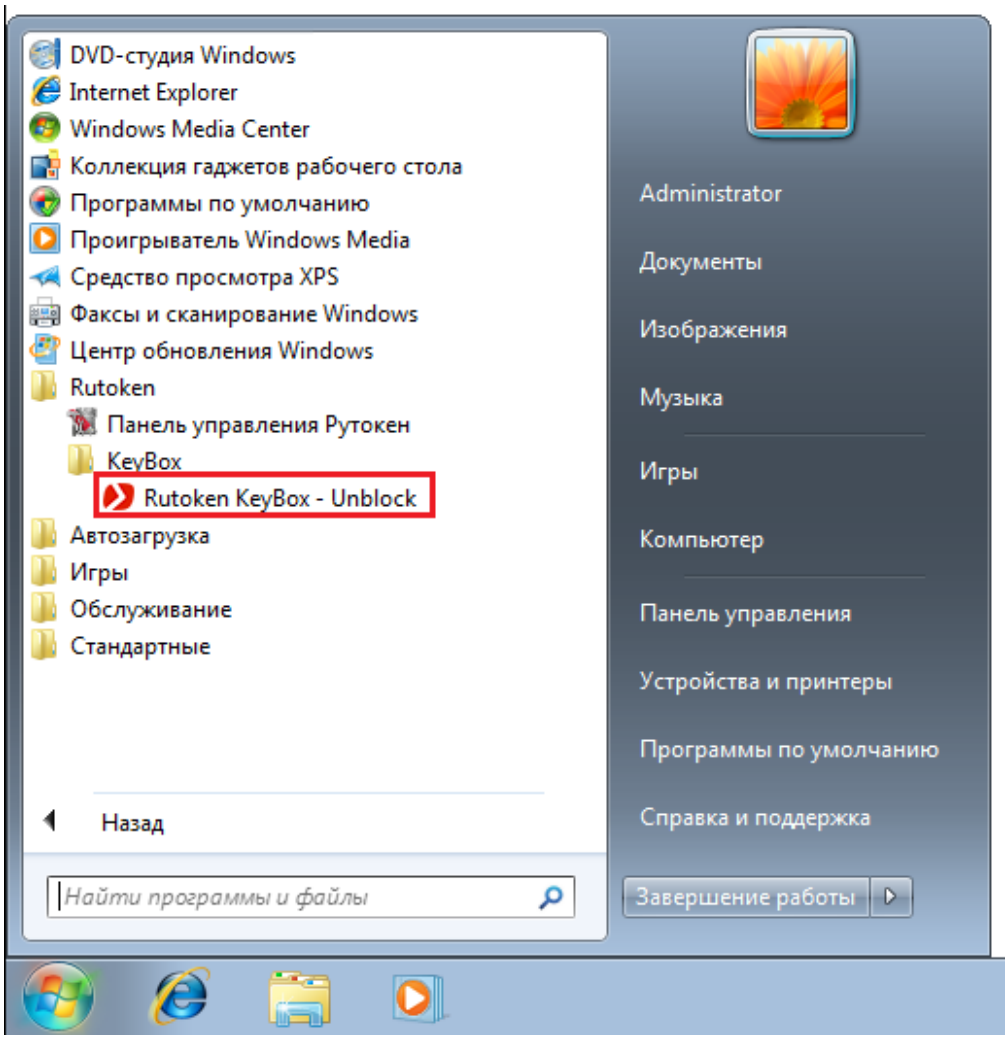
Важная информация

Офлайн-разблокировка может быть запрещена политикой использования устройств.

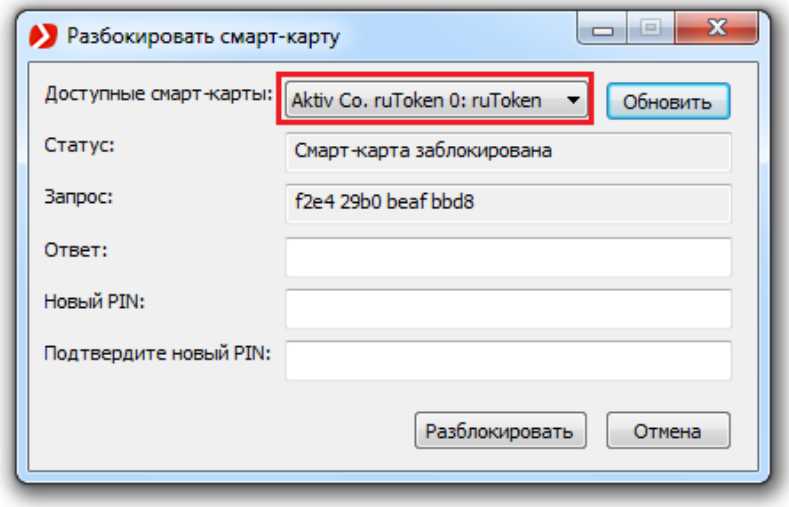
Разблокировка устройства

Для разблокировки устройства:

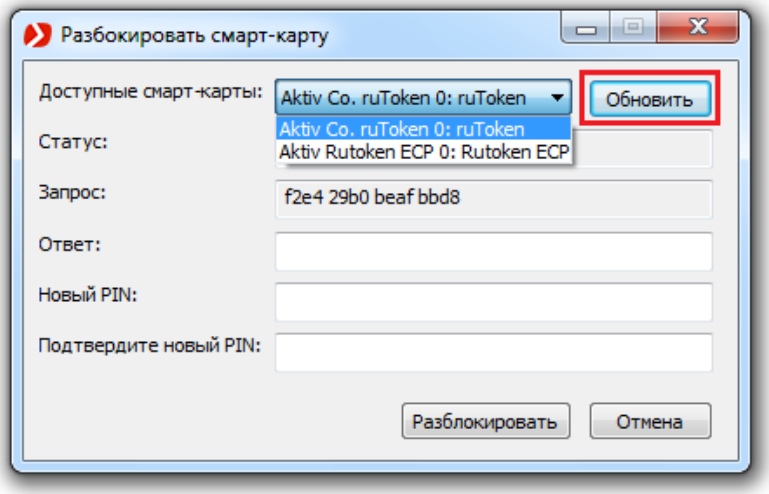
1. Запустите утилиту разблокировки (**Пуск/ Программы/ Rutoken/ KeyBox/ Rutoken KeyBox - Unblock**):



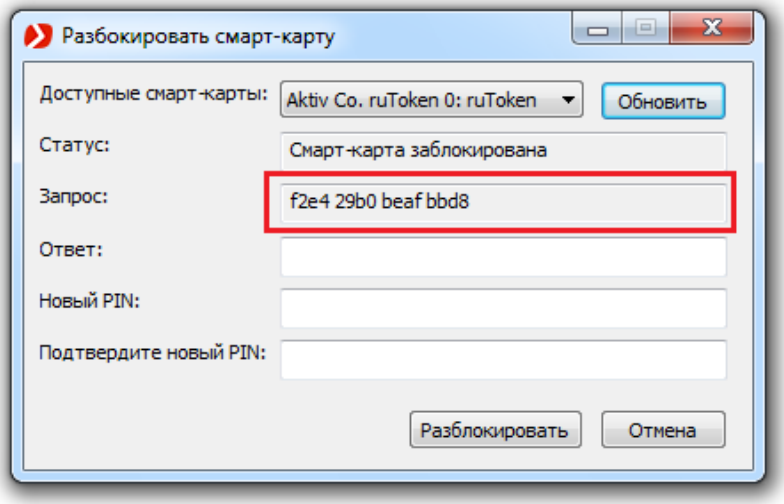
2. Подключите устройство. После подключения утилита обнаружит его автоматически:



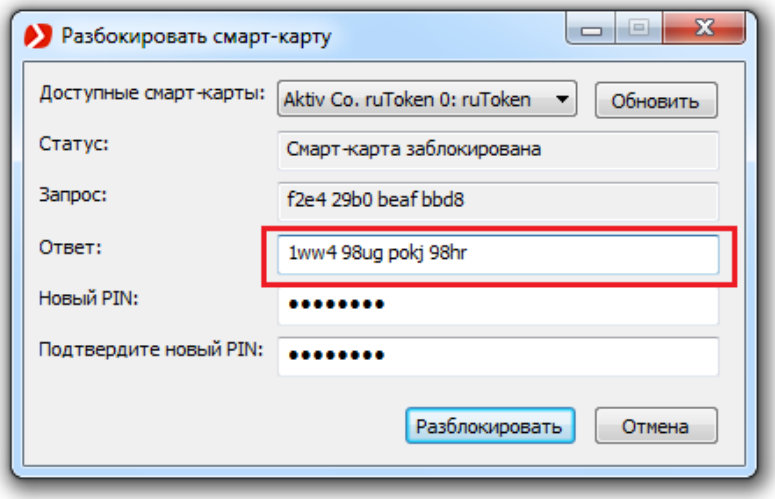
Если подключено несколько устройств, необходимо выбрать нужное устройство из выпадающего списка и нажать на кнопку **Обновить**:



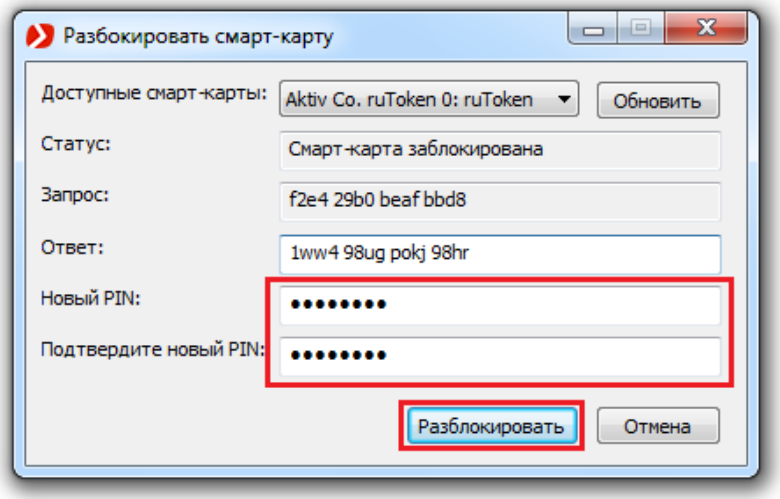
3. В поле **Запрос** будет автоматически сгенерирован запрос на разблокировку устройства. Свяжитесь с сотрудником технической поддержки и сообщите ему запрос.



4. Сотрудник технической поддержки запросит ответы на секретные вопросы для подтверждения личности владельца устройства. В случае корректных ответов сотрудник технической поддержки сообщит код, необходимый для завершения разблокировки устройства. Введите полученый код в поле **Ответ** утилиты разблокировки:



5. Введите новый PIN-код, его подтверждение и нажмите на кнопку Разблокировать:



Устройство будет разблокировано, PIN-код изменен. Значение в поле Статус утилиты изменится на "Смарт-карта не заблокирована":