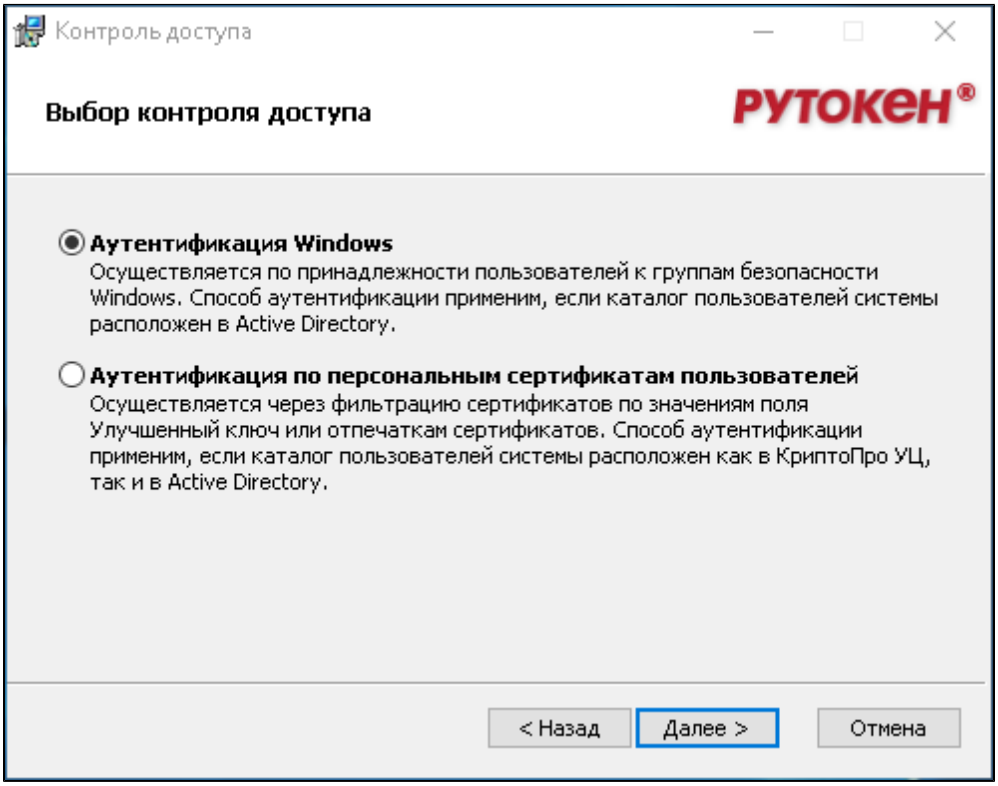
Установка сервера

Запустите файл **RutokenKeyBox.Server.msi** из дистрибутива Рутокен KeyBox (каталог RutokenKeyBox.Server) и выполните установку, следуя указаниям мастера. В процессе установки будет предложено выбрать способ контроля доступа для всех приложений системы.



Система Рутокен KeyBox состоит из набора сервисов:

- **Консоль управления** (Management Console) – веб-приложение **mc**.
- **Сервис самообслуживания** (Self Service) – веб-приложение **ss**.
- **Сервис удаленного самообслуживания за пределами домена** (Remote Self Service) – веб-приложение **rss**.
- **Сервис разблокировки смарт-карт** – веб-приложение **credprovapi**.
- **Сервис API** – веб-приложение **api**.
- **Сервис отслеживания состояния карт** – **Служба Card Monitor**, не имеет веб-приложения.
- Сервисы клиентского агента:
  - **Сервис регистрации агентов** – веб-приложение **agentregistrationapi**.
  - **Сервис агентов для удаленного выполнения задач** – веб-приложение **agentserviceapi**.

Каждый сервис имеет собственные файлы конфигурации и настройки доступа.

Аутентификация Windows

При выборе Аутентификации Windows будут заданы следующие параметры контроля доступа:

- **Проверка подлинности** (Authentication):
  - **Проверка подлинности Windows** (Windows Authentication) для веб-приложений: **Консоль управления** (mc), **Сервис самообслуживания** (ss), **Сервис API** (api). Остальные способы отключены.
  - **Анонимная проверка подлинности** (Anonymous Authentication) для веб-приложений: **Сервис удаленного самообслуживания** (rss), **Сервис разблокировки смарт-карт** (credprovapi), **Сервисов клиентских агентов** (agentregistrationapi, agentserviceapi).
- **Параметры SSL** (SSL Settings):
  - **Требовать SSL** (Require SSL) для всех веб-приложений.
  - **Сертификаты клиента** (Client certificates):
    - **Игнорировать** (Ignore) для веб-приложений: **Консоль управления** (mc), **Сервис самообслуживания** (ss), **Сервис удаленного самообслуживания** (rss), **Сервис разблокировки смарт-карт** (credprovapi), **Сервис API** (api), **Сервис регистрации клиентских агентов** (agentregistrationapi).
    - **Требовать** (Require) для веб-приложения: **Сервис агентов** (agentserviceapi).

Аутентификации по персональным сертификатам пользователей

При выборе Аутентификации по персональным сертификатам пользователей будут заданы следующие параметры контроля доступа:

- **Проверка подлинности** (Authentication):
  - **Анонимная проверка подлинности** (Anonymous Authentication) для всех веб-приложений. Остальные способы отключены.
- **Параметры SSL** (SSL Settings):
  - **Требовать SSL** (Require SSL) для всех веб-приложений.
  - **Сертификаты клиента** (Client certificates):
    - **Игнорировать** (Ignore) для веб-приложений: **Сервис удаленного самообслуживания** (rss), **Сервис разблокировки смарт-карт** (credprovapi), **Сервис регистрации клиентских агентов** (agentregistrationapi).
    - **Требовать** (Require) для веб-приложений: **Консоль управления** (mc), **Сервис самообслуживания** (ss), **Сервис API** (api), **Сервис агентов** (agentserviceapi).

Если каталог пользователей расположен в Active Directory, то сертификаты, используемые для аутентификации должны содержать **User Principal Name**. Без включенного в сертификат **UPN** вход в веб-приложения будет невозможен.

После установки системы **Параметры SSL** для каждого приложения можно изменить вручную в **Диспетчере служб IIS** (IIS Manager).

Для настройки защищенного соединения для веб-приложений, необходимо выпустить SSL/TLS-сертификат и **Привязать** (Bindings) его в **Диспетчере служб IIS** (IIS Manager) для сайта **Default Web Site**:

- Запустите **Диспетчер служб IIS** (Internet Information Services (IIS) Manager).
- Выберите сайт **Default Web Site** и перейдите в раздел **Привязки...** (Bindings...).
- Нажмите **Добавить...** (Add...), выберите **Тип:** (Type:) **https** и **Порт:** (Port:) **443**.
- Выберите **SSL-сертификат:** (SSL certificate:) и нажмите **OK**.

Субъект (Subject) сертификата должен содержать атрибут **Общее имя** (Common name) (FQDN сервера RutokenKeyBox).
Дополнительное имя субъекта (Subject Alternative Name) сертификата должно содержать атрибут **DNS-имя** (DNS Name) (FQDN сервера RutokenKeyBox). Например: *rutokenkeyboxru.demo.local* или соответствующую запись с подстановочными знаками, например: **. demo.local* (Wildcard certificate).
Улучшенный ключ (Enhanced Key Usage) сертификата должен содержать значение **Проверка подлинности сервера** (Server Authentication).