SSO

Технология единого
входа внутри компании
Qoollo

01

Вступление

Наша команда, что такое SSO

Наша команда

Матвей Матвиенко

backend

Элис Суковчева

backend

Даниил Нечитайло

backend

Александр Козаченко

frontend, Саша или Леша?

Наш ментор

Павел пересторонин

Можно просто Паша...

Что такое SSO?

SSO (Single sign-on) - технология, при использовании которой пользователь переходит из одного раздела портала в другой, либо из одной системы в другую, не связанную с первой системой, без повторной аутентификации.

П.с. Википедия не врет

Виды

SAML - язык разметки декларации безопасности.

🗑️ Последнее обновление в 2005 году.

O(pen)Auth 1.0/2.0 - протокол (схема) авторизации.

✔️ 2.0 в 2012 году.
🔓 Реализация потоков (flow) для различный клиентов.
👎 Плохая масштабируемость.

OpenID connect - Децентрализованная система аутентификации.

✔️ 1.0 в 2014 году.
🌐 Расширение OAuth 2.0, менеджер сессий, больше схем flow, можно динамически регистрировать клиентов.
👎 Нереально большая документация.

SSO

Где мы можем увидеть SSO?

Яндекс

Яндекс музыка, яндекс еда, яндекс афиша

Qoollo

Теперь SSO будет и в Qoollo!

Анализ

Существующее решение, решение проблемы

Существующее решение

OpenIDDict

Плюсы:

Реализовано большое кол-во workflow.

Реализация протокола OpenID.

Минусы:

Сложное конфигурирование.

Сложность использования из коробки, как следствие.

Решение проблемы

Собственная реализация SSO

Стек технологий

C#

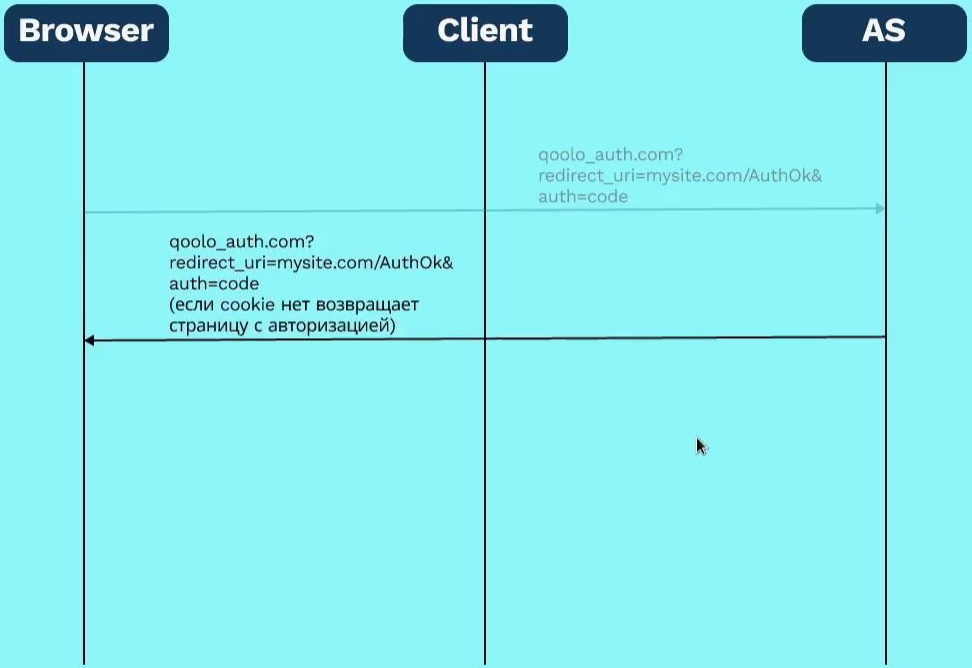
MongoDB

03

Продукт

Разбор схемы работы, демонстрация работоспособности

Разбор схемы работы


Browser
Client
AS
qoolo_auth.com?
redirect_uri=mysite.com/AuthOk&
auth=code
qoolo_auth.com?
redirect_uri=mysite.com/AuthOk&
auth=code
(если cookie нет возвращает
страницу с авторизацией)

Демонстрация работоспособности

Privacy Policy - client one

localhost:5010/Home/Privacy

client one Home Privacy

Privacy Policy

Use this page to detail your site's privacy policy.

Новая вкладка

http://localhost:5020/Home/Privacy

Privacy Policy - client two - http://localhost:5020/Home/Privacy

http://localhost:5020/Home/Privacy - Поиск Google

Сервисы

Список для чтения

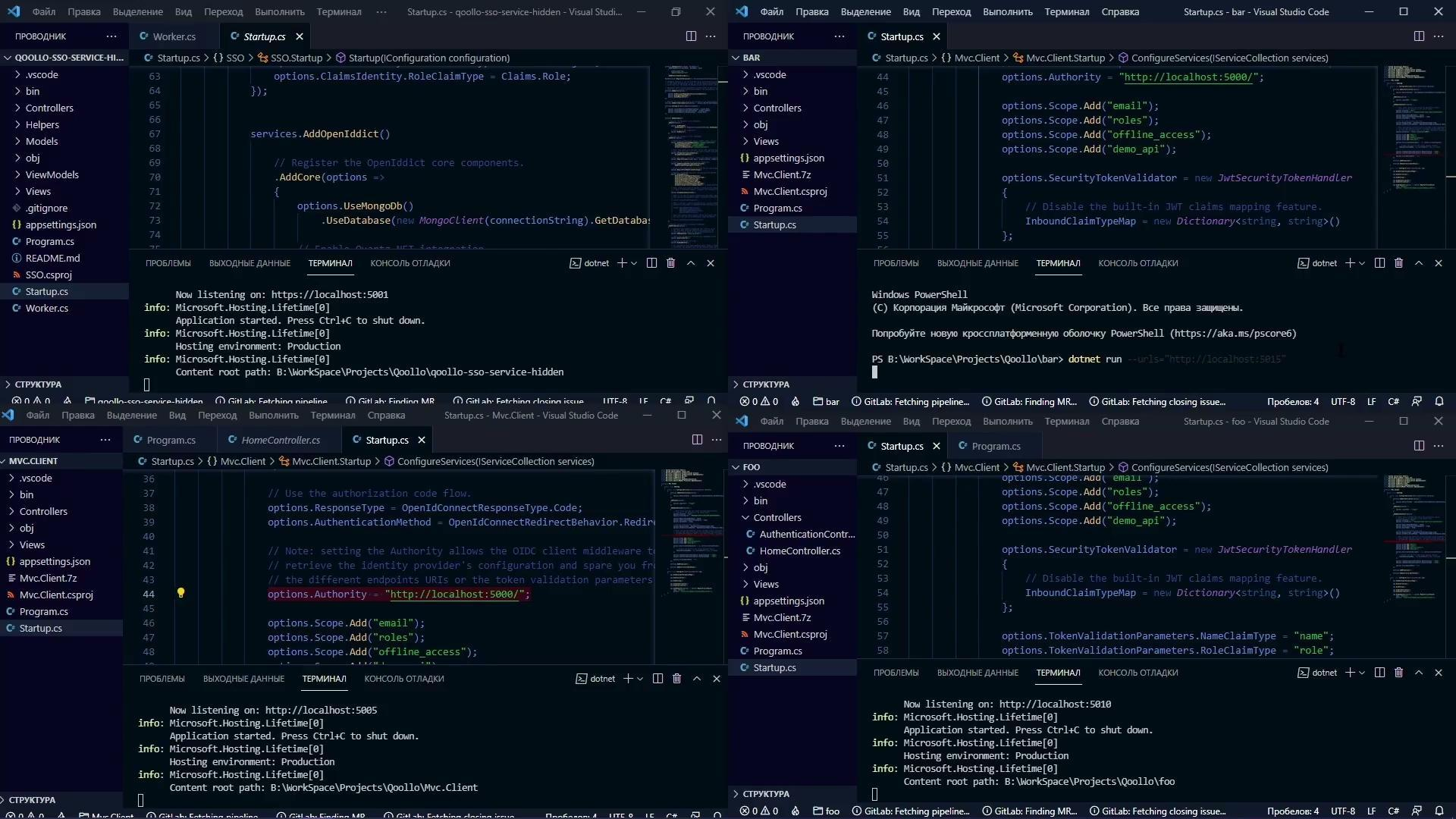
Введите поисковый запрос или URL

vk telegram whatsapp skype github

youtube mail.ru document trello pronto

Настроить

Альтернативная реализация на основе OpenIDDict


Startup.cs - qoollo-sso-service-hidden - Visual Studi...
Startup.cs - bar - Visual Studio Code
Startup.cs - Mvc.Client - Visual Studio Code
Startup.cs - foo - Visual Studio Code
options.ClaimsIdentity.RoleClaimType = Claims.Role;
services.AddOpenIddict()
// Register the OpenIddict core components.
.AddCore(options =>
options.UseMongoDb()
options.Authority = "http://localhost:5000/";
options.Scope.Add("email");
options.Scope.Add("roles");
options.Scope.Add("offline_access");
options.Scope.Add("demo_api");
options.SecurityTokenValidator = new JwtSecurityTokenHandler
// Disable the built-in JWT claims mapping feature.
InboundClaimTypeMap = new Dictionary<string, string>()
// Use the authorization code flow.
options.ResponseType = OpenIdConnectResponseType.Code;
options.AuthenticationMethod = OpenIdConnectRedirectBehavior.Redir
// Note: setting the Authority allows the OIDC client middleware t
// retrieve the identity provider's configuration and spare you fr
// the different endpoints URIs or the token validation parameters
options.TokenValidationParameters.NameClaimType = "name";
options.TokenValidationParameters.RoleClaimType = "role";
Now listening on: https://localhost:5001
info: Microsoft.Hosting.Lifetime[0]
Application started. Press Ctrl+C to shut down.
Hosting environment: Production
Content root path: B:\WorkSpace\Projects\Qoollo\qoollo-sso-service-hidden
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)
PS B:\WorkSpace\Projects\Qoollo\bar> dotnet run --urls="http://localhost:5015"
Now listening on: http://localhost:5005
Content root path: B:\WorkSpace\Projects\Qoollo\Mvc.Client
Now listening on: http://localhost:5010
Content root path: B:\WorkSpace\Projects\Qoollo\foo

04

Заключение

Перспективы, итоги, благодарности

Итоги

Перспективы

Спасибо за практику!