2021

Moduł Obsługi Przychodni

SSO

EGIER MICHAŁ, KWAPIEŃ PAWEŁ, TOBIS BARTOSZ

Spis treści

0. Informacje dodatkowe.

Przedmiot:	Zaawansowane technologie webowe
Nr laboratorium:	12
Grupa:	Czwartek 7:30
Prowadząca:	Mgr. Inż. Maja Kędras
Data:	20.05.2021

1. Przegląd możliwych rozwiązań SSO.

SSO to scentralizowany serwis zarządzający sesją oraz autentykacją, w taki sposób, że pojedynczy zestaw login/hasło może być wykorzystany do uzyskania dostępu do wielu aplikacji. Piękno
tego rozwiązania jest ukryte w jego prostocie. Serwis autentykuje użytkownika na dowolnej platformie,
tym samym w sposób przeźroczysty dla użytkownika dostarcza mu dostęp do wszystkich innych serwisów bez ponownego procesu logowania.

Dostępne rozwiązania SSO:

SAML- Security Assertion Markup Language (SAML) to oparty na języku XML otwarty standard używany do implementacji logowania Single Sign On (SSO). SAML 2.0 został opracowany w 2005 roku i jest aktualną wersją tego standardu. SAML jest używany zarówno do uwierzytelniania, jak i autoryzacji między dwiema stronami: dostawcą usług (Office365, Salesforce, G Suite itp.) i dostawcą tożsamości (Okta, OneLogin, Ping Identity itp.). Z założenia Service Provider (SP) ufa dostawcy tożsamości (Identity Provider- IdP) w procesie uwierzytelniania. Odbywa się to za pomocą dokumentu SAML XML wysłanego przez IdP, zawierającego autoryzację i uwierzytelnienie użytkownika, a następnie przekierowanie do usługodawcy SP.

OAuth2 - to otwarty standard używany do autoryzacji, który umożliwia aplikacjom dostarczanie funkcjonalności z „delegowaną autoryzacją". W przeciwieństwie do innych struktur, które zapewniają uwierzytelnianie, OAuth2 autoryzuje tylko urządzenia, API, serwery z tokenami dostępu, a nie poświadczeniami. Działa przez HTTPS. Technologia OAuth2 powszechnie wykorzystywana jest w takich serwisach jak Facebook czy Google. Serwisy te umożliwiają skorzystanie z ich wewnętrznych mechanizmów autoryzacji do logowania w zewnętrznych serwisach, nie związanych z dostawcą tożsamości.

OpenID Connect- to warstwa tożsamości uzupełniająca protokół OAuth 2.0, która rozszerza OAuth2 i umożliwia „uwierzytelnianie federacyjne" (Federated Authentication). Przebieg procesu OpenID Connect jest podobny do przepływu autoryzacji OAuth2, a główną różnicą jest „token id", który umożliwia uwierzytelnienie użytkownika.

2. Identity Framework.

ASP.NET Core Identity:

- Jest interfejsem API, który obsługuje funkcję logowania interfejsu użytkownika.
- Zarządza użytkownikami, hasłami, danymi profilu, rolami, oświadczeniami, tokenami, potwierdzeniem wiadomości e-mail i nie tylko.

ASP.NET Core Identity:

Jest interfejsem API, który obsługuje funkcję logowania interfejsu użytkownika. Zarządza użytkownikami, hasłami, danymi profilu, rolami, oświadczeniami, tokenami, potwierdzeniem wiadomości e-mail i nie tylko.
Użytkownicy mogą utworzyć konto z przechowywanymi w nim informacjami logowania lub użyć Identity zewnętrznego dostawcy logowania. Obsługiwani zewnętrzni dostawcy logowania to Facebook, Google, Konto Microsoft i Twitter.

Aby uzyskać informacje na temat globalnego wymagania uwierzytelnienia wszystkich użytkowników, zobacz Require authenticated users (Wymaganie uwierzytelnionych użytkowników).

Kod Identity źródłowy jest dostępny w witrynie GitHub. Szkielet Identity i wyświetl wygenerowane pliki, aby przejrzeć interakcję szablonu z programem Identity .

Identity Jest zwykle konfigurowany przy użyciu bazy SQL Server do przechowywania nazw użytkowników, haseł i danych profilu. Alternatywnie można użyć innego magazynu trwałego, na przykład Azure Table Storage.

Jako planowane rozwiązanie przewidujemy wdrożyć IdentityServer 4.

IdentityServer4 jest frameworkiem wykorzystującym OpenID Connect oraz OAuth 2.0 dla aplikacji ASP.NET Core, zatem spełnia wymagania dotyczące wykorzystania SSO w projekcie.