Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004:007
DOI: https://doi.org/10.24867/07OI01Dimic

SISTEM ZA BEZBEDNU KOMUNIKACIJU DVA KORISNIKA PUTEM RAZMENE PORUKA

SECURE MESSAGING COMMUNICATION BETWEEN TWO USERS

Slađana Dimić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – INŽENJERSTVO INFORMACIONIH SISTEMA

Kratak sadržaj – *Cilj ovog rada jeste da se obezbedi sigurna komunikacija u vidu razmene mail-a dva korisnika preko Web aplikacije i Microsoft Outlook-a, klijenta Microsoft Exchange-a. Za ovu komunikaciju potrebno je registrovati novu aplikaciju na Microsoft Azure portalu koja ima identifikatore neophodne za dobavljanje Bearer tokena. Bearer token sluzi da se klijent, u ovom slučaju razvijena Web aplikacija, autentifikuje servisu. Klijent je tada u mogućnosti da, preko Microsoft Graph RESTful Web API-a, potraži sve korisnike određene grupe registrovane na Azure Active Directory-u i pošalje mail odabranom korisniku.*

Ključne reči: *Exchange server, Graph API, Bearer token, RESTful servis, sigurna komunikacija, autorizacija*

Abstract *– The aim of this thesis is to provide secure communication in the form of an email exchange between two users via Web application and Microsoft Outlook, a Microsoft Exchange client. This communication requires a new registered application on the Microsoft Azure portal that has the identifiers that are necessary to deliver the Bearer token. The Bearer token serves to authenticate the client to the service, in this case the client is a developed Web application. The client is then able to, through the Microsoft Graph RESTful API, pull all users of a particular group registered with Azure Active Directory and send mail to the selected user.*

Keywords *– Exchange server, Graph API, Bearer token, RESTful service, secure communication, authorization*

1. UVOD

Platformski *Microsoft* servis *Azure Active Directory* daje mogućnost kompanijama širom sveta da skladište svoje podatke na *Cloud*, radi povećanja kapaciteta skladištenja podataka i obezbeđenja sigurnosti podataka. Kompanije tako, pored ostalih podataka, skladište podatke o svim korisnicima, odnosno članovima kompanije. Kako je svaka kompanija podeljena u više sektora, kao što su na primer sektor razvoja, sektor prodaje, sektor finansija i slično, tako svaki korisnik pripada određenoj grupi, odnosno sektoru. Neke kompanije današnjice imaju svoj softver kroz koji vode poslovanje. Kako bi zaposleni kompanije i njeni korisnici komunicirali uz pomoć softvera, odnosno razvijene *Web* aplikacije slanjem *mail*-a na željeni *Microsoft Outlook* nalog, tako da komunikacija bude sigurna operacija, potrebno je registrovati novu aplikaciju na *Microsoft Azure* portalu i dodeliti joj permisije koje će u nastavku teksta biti opisane. Preko takve registrovane aplikacije, kompanijska *Web* aplikacija bila bi u mogućnosti da potraži *Bearer token* koji služi za autentifikaciju servisu. Sa dobijenim *Bearer token*-om kompanijska *Web* aplikacija preko *Microsoft Graph API*-a i *RESTful* servisa predefinisanim upitom može da potraži sve korisnike određene grupe. Nakon što dobije korisnike, takođe preko *Microsoft Graph API*-a i *RESTful* servisa uz pomoć *Bearer* autentifikacije može da pošalje *mail* odabranim korisnicima u ime željenog korisnika. Za povlačenje korisnika određene grupe potreban je identifikator grupe, dok je za slanje *mail*-a u ime određenog korisnika potreban identifikator korisnika iz *Active Directory*-a. Ovim pristupom se izbegava lokalno čuvanje podataka korisnika koje zauzima memoriju, obezbeđuje sigurnost podataka kojima ne može svako da pristupi, kao i zloupotreba podataka.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Srđan Sladojević, vanr. profesor.

2. PREGLED RELEVANTNE LITERATURE

2.1. Microsoft Exchange Server

Microsoft Exchange je u osnovi *mail* server razvijen od strane *Microsoft*-a koji, između ostalog, podržava i svoj klijent *Outlook*. *Exchange* omogućava korisnicima da razmenjuju informacije pomoću *Outlooka* ili *Outlook Web Accessa*, dakle omogućava saradnju među korisnicima. Od verzije *Exchange* 2000, *Exchange* više nema svoj *directory* servis, već se kompletno oslanja na *Active Directory* infrastrukturu. *Exchange* je teško konfigurisati pa ga manje firme ne implementiraju, ali ta kompleksnost poseduje funkcije koje su važne za povezivanje nekoliko hiljada *Exchange* korisnika [1].

2.2. Microsoft Outlook

Microsoft Outlook je *Microsoft* aplikacija za *email*, koja takođe uključuje kalendar, koordinisanje zadacima, menadžer kontakata, beleške, dnevnik i *Web* pregled. Može se koristiti kao samostalna aplikacija ili može raditi sa *Microsoft Exchange* serverom za vise korisnika u organizaciji [2].

2.3. Microsoft Azure Active Directory

Azure je *Microsoft* platforma za *Cloud* koja omogućava hostovanje aplikacija i čuvanje dokumenata.
Active directory je servis kreiran od strane *Microsoft*-a, koji čuva informacije o objektima na mreži tako da im autentifikovani korisnici kao i administratori mreže u svakom trenutku mogu lako pristupiti [3].

2.4. Microsoft Cloud

Cloud podrazumeva skladištenje podataka na internetu, a ne lokalno na *hard disk drive*-u. Nije reč samo o podacima, skladište se i kompletni sistemi, potreban je samo izlaz na internet.

2.5. REST arhitektura

REST (*Representational state transfer*) arhitekturalni stil je set principa koji definiše kako bi *Web* standardi poput *HTTP (Hypertext Transfer Protocol)* i *URI* (*Uniform Resource Identifier*) trebali da se koriste. Ipak, na programerima i arhitektama je da ga održe uniformnim. Nije zavistan ni od jednog protokola, ali gotovo svaki *RESTful* servis koristi *HTTP/HTTPS (Hypertext Transfer Protocol Secure)* kao osnovni protokol pa tako, *REST* označava način komunikacije između klijenta i servera korišćenjem mrežnih resursa pomoću *HTTP* protokola. Američki naučnik Roj Filding (*Roy Fielding*) je u svojoj doktorskoj disertaciji [4] prvi put pomenuo pojam *REST* gde je rekao da je motivacija za razvoj *REST*-a pravljenje modela arhitekture koji opisuje kako bi *Web* trebalo da radi, takvog da može da posluži kao orijentir pri definisanju standarda protokola za *Web*.

2.6. RESTful servis

RESTful servisi su zasnovani na *REST* arhitekturi i dobro su integrisani sa *HTTP* protokolom. Ne zahtevaju *XML (Extensible Markup Language)* poruke kao ni *WSDL (Web Services Description Language*) definiciju. Prilično je jednostavan za korišćenje (*human readable*) i važi da dominantan mrežni servis današnjice. Podaci se najčešće razmenjuju u *JSON*, *XML* i *YAML* formatima. Može biti izvršen na bilo kom klijentu ili serveru koji ima *HTTP/HTTPS* podršku. Kod ovog tipa servisa, resursi (npr. statičke strane, fajlovi, podaci iz baze...) imaju sopstveni *URL* (*Uniform Resource Locator*) ili *URI* (*Uniform Resource Identifier*) koji ih identifikuju. Pristup do resursa je definisan *HTTP* protokolom, gde svaki poziv čini jednu akciju (kreira, čita, menja ili briše podatke). Isti *URL* se koristi za sve operacije ali se menja *HTTP* metod koji definiše vrstu operacije. *REST* koristi *Create, Read, Update, Delete* (*CRUD*) *HTTP* metode kao što su: *GET, POST, PUT, DELETE* [5]. Skoro svi veliki *Web* servisi kao što su *Google*, *Twitter* i *Facebook* se oslanjaju na *REST* arhitekturu za njihov *API* (*Application programming interface*), zato što *HTTP* protokol pokreće skoro sve internet konekcije. Klijent i servis ne moraju da budu u uskoj vezi prilikom razmenjivanja poruka, pa tako sve informacije koje se prenose kao resursi staju u jedinstveni identifikator *URI* koji je kao takav dovoljan za razumevanje zahteva. Ukoliko klijent i servis žele da komuniciraju na siguran način, *Header* sekcija *HTTP* zahteva podržava vid autorizacije putem *Bearer token*-a koji *Microsoft* obezbeđuje, što predstavlja jedan od načina sigurne komunikacije.

2.7. Microsoft Graph API

Microsoft Graph je *RESTful Web API* koji omogućava pristup resursima *Microsoft Cloud* usluge. Nakon što se registruje aplikacija i dobije *token* za autentifikaciju za korisnika ili uslugu, mogu se podnositi zahtevi za *Graph API*. *Graph API*-u se pristupa *HTTP* metodama, najčešće su *POST, GET, PUT* i *DELETE* metode koje opisuju *CRUD* (*Create, Read, Update, Delete*) operacije [5].

2.8. Bearer autentifikacija

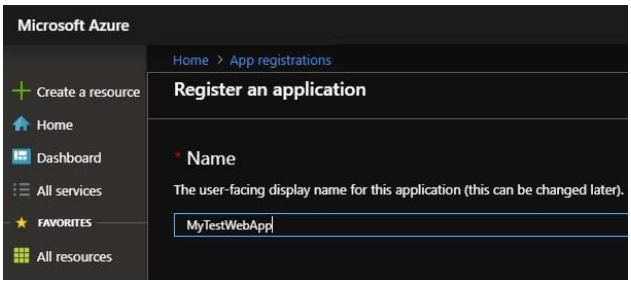
Bearer autentifikacija kao provera identiteta nosioca, odnosno provera identiteta *token-a*, je *HTTP* šema provere autentičnosti *Bearer token*-a. *Bearer* autentifikacija se može shvatiti i kao davanje pristupa nosiocu ovog *token*-a. *Bearer token* je kriptovani *string* koji je uglavnom generisan od strane servera kao odgovor na zahtev. Klijent dobijeni *token* šalje kroz zaglavlje autorizacije prilikom definisanja *HTTP* zahteva [6].

3. OPIS FUNKCIONALNOSTI

U ovom poglavlju će biti predstavljena registracija nove aplikacije na *Microsoft Azure* portalu, koja će razvijenoj klijentskoj *Web* aplikaciji omogućiti *Bearer token* preko *Microsoft*-a, kako bi razvijena *Web* aplikacija korišćenjem *Bearer token*-a mogla da povuče informacije o svim korisnicima određene grupe *HTTP* upitom na *Microsoft Graph API*, zatim poslati *mail* odabranom korisniku.

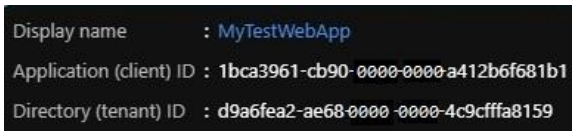
3.1. Registrovanje aplikacije na Azure portalu

Svako ko ima poslovni ili privatni *Microsoft* profil može da se registruje na *Microsoft Azure* portal i registruje svoju *Web* aplikaciju (Slika 1).

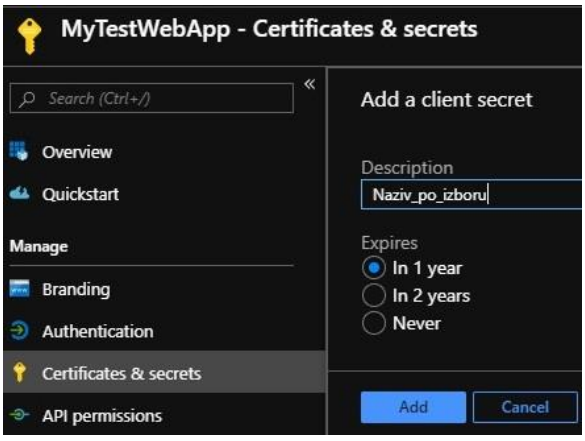


Slika 1. *Registrovanje nove aplikacije na Azure*

Prilikom registrovanja aplikacije, automatski se dodeljuje *identifikator aplikacije* od strane *Microsoft*-a. Za dobavljanje *Bearer token*-a potrebni su *application id* koji se automatski generiše, *domain* (*tenant) id* (Slika 2) koji se može videti nakon prijave korisnika na *Azure* portal i *Client secret* lozinka koju korisnik sam mora da generiše (Slika 3).

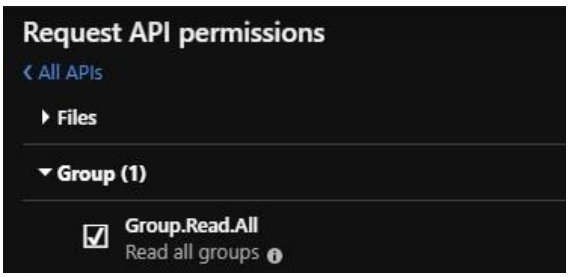


Slika 2. *Client ID i Tenant ID*

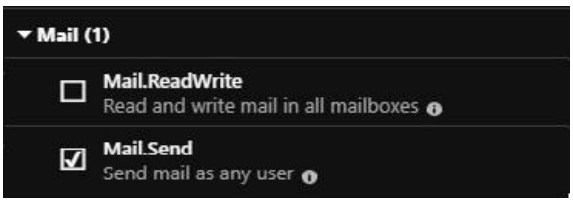


Slika 3. *Generisanje Client secret lozinke*

Postoje *Microsoft Graph* permisije koje omogućavaju korišćenje *Microsoft Graph API*-a i koje se dele na aplikativne permisije (*application permissions*) i delegirane (*delegated permissions*). Aplikativne permisije su za klijente, a delegirane za korisnike. Kako je registrovana aplikacija na *Azure* portalu klijent, trebaju da joj se dodele aplikativne permisije za čitanje svih korisnika određene grupe (Slika 4) i aplikativne permisije za slanje mail-a umesto bilo kog korisnika (Slika 5).

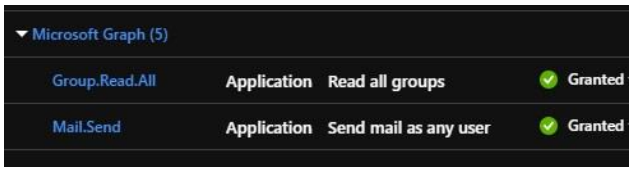


Slika 4. *Aplikativne permisije za čitanje podataka grupe*



Slika 5. *Aplikativne permisije za slanje mail-a kao klijent*

Nakon odabira permisija, iste moraju biti odobrene od strane administratora (Slika 6).



Slika 6. *Odobrene aplikativne permisije od strane administratora*

3.2. Dobavljanje Bearer tokena sa Microsoft Exchange servera

Prilikom pokretanja razvijene *Web* aplikacije, aplikacija šalje upit na *Microsoft* preko *RESTful* servisa putem *HTTP POST* metode. Za slanje zahteva potrebni su *application id* od registrovane aplikacije na *Azure* portalu, *Clent secret* lozinka i *domain id* (Slika 7) [7].

```
POST https://login.microsoftonline.com/{tenant}/oauth2/v2.0/token HTTP/1.1
Host: login.microsoftonline.com
Content-Type: application/x-www-form-urlencoded

client_id=535fb089-9ff3-47b6-9bfb-4f1264799865
&scope=https%3A%2F%2Fgraph.microsoft.com%2F.default
&client_secret=qWgdYAmab0YSkuL1qKv5bPX
&grant_type=client_credentials
```

Slika 7. *Primer HTTP POST zahteva za dobijanje access Bearer token-a*

Aplikacija zatim dobija odgovor o podacima *Bearer tokena* u *JSON* formatu gde se može videti koji je tip *token*-a, kada ističe i sam kriptovan *string* koji služi za autentifikaciju (Slika 8).

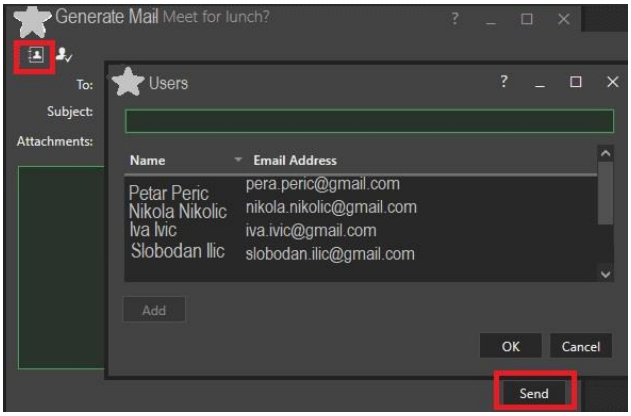
```
{
  "token_type": "Bearer",
  "expires_in": 3599,
  "access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ik1uQ19WWmNBVGZNNXBP..."
}
```

Slika 8. *Odgovor na zahtev potraživanja tokena*

Token se potražuje ponovo nakon isteka definisanog vremena *expires_in* u odgovoru.

3.3. Povlačenje svih korisnika određene grupe pomoću Bearer tokena

Nakon iniciranja komunikacije od strane razvijene *Web* aplikacije u cilju definisanja *mail*-a, automatski se povlače svi korisnici određene grupe iz *Active Directory*-a tako da se u novootvorenom prozoru klikom na *icon* „*Get Users*“ može videti lista dobijenih korisnika (Slika 9).



Slika 9. *Lista povučenih korisnika iz Active directory-a*

Prilikom slanja zahteva na *Microsoft Graph API* u cilju povlačenja svih korisnika određene grupe, kroz *Header Authorization* zaglavlje se šalje prethodno dobijeni *Bearer token*, a kroz *URL* zahteva putem *HTTP GET* metode šalje se identifikator grupe (Slika 10).

```
var request = (HttpWebRequest)WebRequest.Create
    ("https://graph.microsoft.com/v1.0/groups/00000000-0000-0000-0000-example00000/members");
request.ContentType = "application/json";
request.Method = "GET";
var token = _clientTokenManager.Get();
request.Headers["Authorization"] = "Bearer " + token.GetAccessToken();
var response = (HttpWebResponse)request.GetResponse();
```

Slika 10. *HTTP GET zahtev za dobavljanje korisnika preko Microsoft Graph API-a, sa Bearer autentifikacijom*

3.4. Slanje mail-a odabranim korisnicima pomoću Bearer tokena

Nakon odgovora od strane *Microsoft Graph API*-a o potraživanju korisnika određene grupe, krajnji korisnik aplikacije selektuje korisnike kojima želi da pošalje generisani *mail*. Klikom na dugme „*Send*“ (Slika 9) inicira se slanje *mail*-a koje se takođe kao i dobavljanje korisnika vrši preko *Microsoft Graph API*-a, slanjem *HTTP POST* zahteva sa definisanim *Header Authorization token*-om i sadržajem *mail*-a u *body* segmentu *HTTP POST* zahteva. *URL HTTP POST* zahtev sadrži identifikator korisnika koji šalje mail (Slika 11).

```
var request = (HttpWebRequest)WebRequest.Create
    ("https://graph.microsoft.com/v1.0/00000000-0000-0000-0000-example00000/sendMail");
request.ContentType = "application/json";
request.Method = "POST";
var token = _clientTokenManager.Get();
request.Headers["Authorization"] = "Bearer " + token.GetAccessToken();

using (var streamWriter = new StreamWriter(request.GetRequestStream()))
{
    streamWriter.Write(jsonEmail);
    streamWriter.Flush();
    streamWriter.Close();
}

var response = (HttpWebResponse)request.GetResponse();
```

Slika 11. *HTTP POST zahtev za slanje mail-a korisnika preko Microsoft Graph API-a, sa Bearer autentifikacijom*

4. ZAKLJUČAK

U ovom radu opisano je razvijeno rešenje za sigurnu komunikaciju korisnika jednog softvera koji u sklopu svog rešenja ima podršku za slanje *mail*-a na *Microsoft Outlook* nalog. Sigurna komunikacija se obavlja uz pomoć *Microsoft Bearer token*-a koji služi za autentifikovanje klijenta servisu. Za povlačenje tokena sa *Microsoft*-a, potrebno je poslati *HTTP POST* zahtev koji sadrži identifikatore koji se dobijaju iz registrovane aplikacije na *Azure* portalu.

Uslov za povlačenje svih korisnika određene grupe sa *Azure Active Directory*-a i slanje *mail*-a u ime željenog korisnika jeste da kompanija svoje podatke o korisnicima (*Users*) i grupama skladišti na *Cloud* i da registrovanoj aplikaciji na *Azure* dodeli aplikativne permisije za čitanje korisnika grupe i slanje *mail*-a u ime bilo kog korisnika.

Aplikacija koja je realizovana za potrebe povlačenja *Bearer token*-a i korisnika, kao i za slanje *mail*-a pisana je u razvojnom okruženju *Microsoft Visual Studio 2015*.

Predstavljenim rešenjem kompanija oslobađa lokalnu memoriju od čuvanja podataka koje može da skladišti na *Cloud* i uvodi veću sigurnost podakata kojima ne može svako da pristupi. Pored toga, korisnici mogu centralizovano, samo preko Web aplikacije, da vode svoje aktivnosti.

Kao veći vid sigurnosti razmene podataka na registrovanu aplikaciju se mogu uvesti i sertifikati. Pored čitanja korisnika i slanja *mail*-a, *Microsoft* nudi i mnoge druge operacije kao što su čitanje *mail*-ova korisnika koje mogu biti i po nekom kriterijumu, čitanje osnovnih podataka o kompaniji, praćenje osnovnih događaja kompanije i mnoge druge opcije koje kompanija dozvoli deljenjem podataka na *Cloud*.

5. LITERATURA

[1] Wikipedia, „Microsoft Exchange Server,“, 9 September 2019. Dostupno: https://en.wikipedia.org/wiki/Microsoft_Exchange_Server. [Poslednji pristup Avgust 2019].

[2] Wikipedia, "Wikipedia Outlook", September 2019. Dostupno: https://en.wikipedia.org/wiki/Microsoft_Outlook. [Poslednji pristup Septembar 2019].

[3] Microsoft, „What is Azure Active Directory,“ Microsoft Azure, Dostupno: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis. [Poslednji pristup Septembar 2019].

[4] Roy Fielding, Architectural styles and the design of network-based software architectures. Vol. 7. Doctoral dissertation, California, Irvine: University of California, 2000.

[5] Mumbaikar, Snehal, and Puja Padiya, „"Web services based on soap and rest principles.", *International Journal of Scientific and Research Publications*, 2013.

[6] Swagger, „Bearer Authentication,“ 2019. Dostupno: https://swagger.io/docs/specification/authentication/bearer-authentication/. [Poslednji pristup Avgust 2019].

[7] Microsoft, "Get access without a user", Microsoft Graph. Dostupno: https://docs.microsoft.com/en-us/graph/auth-v2-service. [Poslednji pristup Septembar 2019].

Kratka biografija

Slađana Dimić rođena je u Novom Sadu 1993. godine. Diplomirala je na Fakultetu tehničkih nauka u Novom Sadu na departmanu za Industrijsko inženjerstvo i menadžment 2016. godine i iste godine upisala master studije na smeru Inženjerstvo informacionih sistema na Fakultetu tehničkih nauka.