ISAM INTEGRACIJA SA FACEBOOK PLATFORMOM KAO PROVAJDEROM IDENTITETA PREKO OPENID CONNECT PROTOKOLA

Bojan Bucalo*,
Jovana Samardžija,
Saša Adamović

Univerzitet Singidunum,
Beograd, Srbija

Rezime:

IBM Security Access Manager (*ISAM*) je *web access* rešenje koje omogućava autentifikaciju, autorizaciju, upravljanje sigurnošću kao i centralizaciju resursa. *IBM Security Access Manager* poseduje modul federacije kako bi saradničke kompanije mogle da pruže međusobno siguran pristup različitim aplikacijama. Korišćenjem federacije, dobija se sigurna, bešavna prijava stranoj aplikaciji, čime se izbegava potreba za višestrukim korisničkim nalozima. Po definiciji, federacija je veza u kojoj obe strane prihvataju korišćenje istog tehničkog standarda pri tom omogućavajući obostrani pristup resursima i podacima. Sastoji se od više provajdera servisa kao i od jednog provajdera identiteta. *Facebook platforma* kao jedan od najvećih provajdera identitetima na svetu je kompatibilna i omogućava vezu, odnosno poverenje prema ISAM rešenju.

Ključne reči:

Web Access, ISAM, Federacija, Facebook platforma, OAuth 2.0, OpenID Connect.

1. IBM SECURITY ACCESS MANAGER

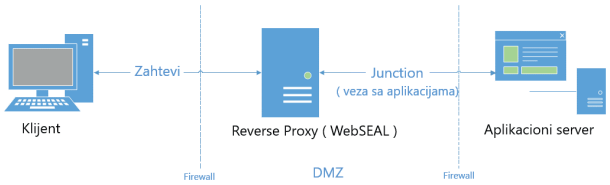
IBM Security Access Manager (ISAM) je *web access* rešenje koje pomaže da se pojednostavi pristup korisnika dok se bezbednije usvajaju *web*, *IOT (Internet Of Things)* i *cloud* tehnologije. Usled svoje fleksibilnosti može se koristiti u lokalnom, virtuelnom i hardverskom okruženju ili se pak može koristiti i u kontejnerima sa *Docker* platforme. *ISAM* pomaže da uspostavimo ravnotežu između upotrebljivosti i bezbednosti kroz korišćenje pristupa zasnovanog na jednostrukoj prijavi, riziku, integrisane kontrole pristupa, federacije identiteta kao i mobilne više faktorske autentifikacije.

Uspostavljanje upravljanja i kontrole sa *IBM SAM* rešenjem i njegov proces bi slikovito izgledao ovako:

Odgovorno lice:
Bojan Bucalo

e-pošta:
bojan.bucalo.15@singimail.rs

DOI: 10.15308/Sinteza-2019-250-255



Slika 1. ISAM arhitektura

2. FEDERACIJA

Federacija kao veza u kojoj obe strane prihvataju korišćenje istog tehničkog standarda pri tom omogućavajući obostrani pristup resursima i podacima takođe pruža mogućnost korišćenja mnogih funkcija kao što su: [1]

- *Federated single sign-on (SSO)* za korisnike višestrukih aplikacija
- Podrška za SAML 2.0, WS-Federacija *(Web Service Federation)*, kao i OAuth 2.0 odnosno *OpenID Connect* protokol za pristup putem federacije
- Prethodno integrisana rešenja federacije putem konektora za popularne *cloud* aplikacije

Federacija je grupa mrežnih ili računarskih provajdera koji se dogovaraju o standardima rada uz obostranu korist. Termin se može koristiti za opisivanje međusobnog funkcionisanja dve različite, formalno nepovezane, telekomunikacione mreže koje mogu imati različite unutrašnje strukture. Da bi dve strane bile u federaciji neophodno je da komunikacija između dveju mreža bude moguća i stabilna.

3. OAUTH 2.0

OAuth2.0 je protokol industrijskog standarda za autorizaciju. Nasledio je i u potpunosti zamenio svog prethodnika koji je nastao 2006. godine. Prvi put se pojavio kao verzija OAuth1.0 2006. godine kada je rađen kao OpenID rešenje za *Twitter*. Nakon nekoliko godina prvi put je i objavljen kao standard 2010. godine da bi samo dve godine kasnije objavljena i verzija OAuth2.0.

OAuth2.0 je poseban po svojim specifičnim procesom autorizacije za veb aplikacije kao i desktop, mobilne pa čak i *IOT* uređaje.[2] Koristi se kao način da se korisnicima interneta omogući pristup veb stranicama odnosno njihovim veb aplikacijama kao i informacijama sa sistema bez delegiranja lozinke. Velike kompanije kao što su *Facebook, Amazon, Google, Twitter, Microsoft* kako bi proširili mogućnosti svojim korisnicima da pomoću svojih naloga pristupaju stranim aplikacijama (aplikacijama koje nisu vezane za njihove servise) su ga uvrstile kao svoju uslugu. Zasnovan je na SOAP odnosno REST protokolu razmene poruka. Predstavljanje toka informacija u jednom OAuth procesu bi izgledalo ovako.

Komunikacija između klijenta i autorizacionog servera:

Traži dozvolu

- K=>AS “Ćao, treba mi pristup tvojoj aplikaciji ” (Autorizacioni zahtev) PK

Traži identifikaciju (korisničko ime i lozinku) i šalje nekakav izazov (npr. otp,…)

- AS=>K “Predstavi se, ko si ti ?” (Autorizacija, Dozvoljeno) PK

Identifikuje se i rešava izazov i dostavlja ga AS

- K=>AS “Ja sam k.i.:client lozi:client, evo otp (Autorizacija, Dozvoljeno) ZK

Obezbeđuje *access token*

- AS=>K “OK, možeš pristupiti aplikaciji” (*Access Token*) ZK

Koristi *token* da pi pristupio resursu

- K=>RS “Pita za korišćenje resursa” (*Access Token*) PK

Identifikuj *token* i dozvoli korišćenje resursa

- RS=>K “Vraća resurs” (Zaštićeni resursi) PK

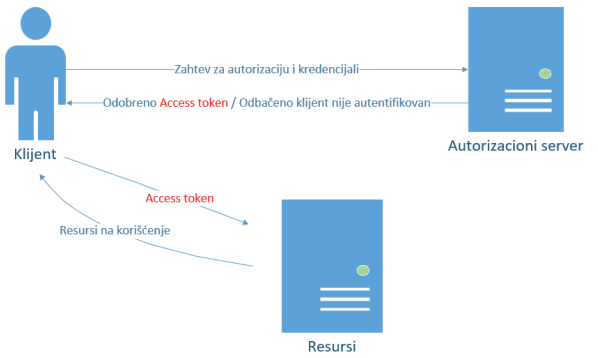
K = Klijent

AS = Autorizacijoni Server

ZK= Zadnji kanal

PK= Prednji kanal

Dva kanala se koriste da bi se povećala sigurnost. Grafički prikazano to bi izgledalo ovako:



Slika 2. Proces OAuth protokola

4. SOAP I REST PROTOKOL

SOAP je protokol koji u sebi sadrži niz važnih pravila i uz pomoć njih postiže nivo standardizacije, dok za razliku od njega REST protokol ima složeniju arhitekturu i fleksibilniji je po tom pitanju. Ujedno SOAP i REST imaju dobro predefinisana pravila koja im omogućavaju uspešnu razmenu informacija. Kada nekad u životu postavimo sebi pitanje: "Kako da pristupimo veb servisima?" odgovor bi bio prost korišćenjem Simple Object Access Protocol (SOAP) ili pak korišćenjem Representational State Transfer (REST).

Upoređivanje SOAP sa REST protokolom

Prednosti SOAP protokola:

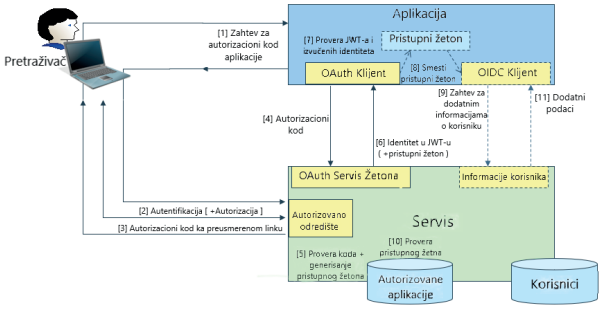
- Nezavisnost jezika, platforme i transporta (REST zahteva upotrebu HTTP-a)
- Dobro funkcioniše u distribuiranim poslovnim okruženjima (ko REST-a se pretpostavlja direktna komunikacija od tačke do tačke)
- Standardizovan
- Ugrađeno rukovanje greškama
- Kada se koristi sa specifičnim jezičnim proizvodima postoji automatizacija

Prednosti REST protokola:

- Nisu potrebni skupi alati za interakciju sa veb uslugama
- Jednostavniji je za korišćenje samim tim se i brže uči
- Efikasnost (SOAP zahteva upotrebu XML za sve poruke, dok REST može da koristi i poruke u manjim formatima)
- Brzina (nema zahtevnih obrada)
- Izuzetno blizu veb tehnologijama u filozofiji dizajna

5. OPENID CONNECT

OpenID Connect je protokol koji u svojoj osnovi zasnovan na OAuth 2.0 protokolu s tim što je dodato par modifikacija odnosno novina. Glavna novina jeste ta da je na postojeći OAuth protokol dodat takozvani *identity layer* ili drugačije rečeno omogućeno je da klijenti verifikuju identitet krajnjeg korisnika na osnovu autentifikacije izvršene od strane autorizacionog servera kao i da dobiju osnovne informacije o krajnjem korisniku i sve to zasnovano na REST protokolu. Ako ste upoznati sa SAML protokolom, OpenID Connect struktura je izuzetno slična osim što OpenID Connect koristi REST odnosno JSON format dok SAML protokol koristi isključivo XML tip poruke.



Slika 3. Proces OpenID Connect protokola [3]

6. FACEBOOK

Facebook je društvena mreža nastala 2004. godine koja svojim korisnicima iz godine u godinu pruža sve više usluga i mogućnosti, pa tako i servise *Facebook* platforma i *Facebook Connect* koje će nama poslužiti za ovaj slučaj.

Facebook platforma

Facebook platforma je platforma društvene mreže *Facebook* koja pruža skup usluga, servisa, alata i proizvoda kao spoljno lice programerima koji za svoje aplikacije žele da pristupaju *Facebook* podacima. Nastala je 2010. godine, i do sad se razvila toliko da pruža programerima širok asortiman interfejsa i alata za olakšan rad. Neki od tih alata su "social graph", "Log In with Facebook", … Iz pogleda programera *Facebook* platforma se ponaša kao treće lice od poverenja, koje omogućava dodatne opcije i olakšice. Ovaj princip je jako koristan i programeri se često odlučuju za njega pogotovo oni koji se bave veb programiranjem. Povezivanjem svoje veb aplikacije sa *Facebook* platformom omogućuju svojim korisnicima prijavu na njihov sajt bez pravljenja dodatnog naloga, jedino što treba da imaju je *Facebook* nalog i moći će da pristupe toj aplikaciji.[4]

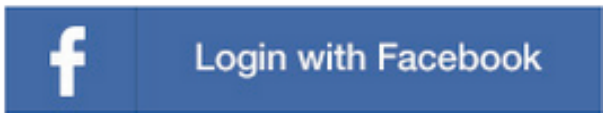
Facebook Connect

Facebook Connect još poznatiji i kao *Log in with Facebook* je skup *API*-ja koji za programere pružaju

uslugu autentifikacije sa *Facebook*-om i da njihovi korisnici mogu da se povežu i podele sa *Facebook* prijateljima. Kao takav *Facebook Connect* pruža da *Facebook* korisnici mogu da se prijave na spoljne veb aplikacije, aplikacija, mobilnih uređaja i sistema i ujedno svoje bitisanje na istim mogu ažurirati odnosno objavljivati na svojim *Facebook* profilima, deliti sa svojim prijateljima kao i pratiti statistike svojih aktivnosti.[5]

7. INTEGRACIJA FACEBOOK-A SA ISAM REŠENJEM

IBM Security Access Manager kao samostalni proizvod može da vrši usluge provajdera identitetima i u standardnim okruženjima to i radi. Međutim u velikom broju okruženja i platformi klijenti prilikom zahteva za ISAM rešenje koji će da štiti njihove aplikacije, traže da provajder identiteta bude neki spoljašnji provajder (*third-party provider*). Najčešće su to *Google, Facebook, Outlook, Linked In*, … U našem slučaju imamo neku javno dostupnu stranu koja je socijalnog karaktera tako da nam je najpovoljnija opcija bila da taj spoljašnji provajder identiteta bude baš *Facebook*. Sigurno ste negde videli ovaj vid obezbeđivanja identiteta za prijavu.



Slika 4. Dugme za korišćenje Facebook-a kao provajdera [6]

Ljudi se često odlučuju prilikom svoje prijave na veb stranice da im Facebook bude provajder naloga jer nemaju vremena da naprave nalog baš za tu stranicu i posao koji žele da obave na toj stranici ne istiskuje toliko vremena ili jednostavno žele trenutno korišćenje te veb stranice i ne žele da prave trajne naloge a kad već imaju Facebook nalog to im dođe kao odličan izbor koji radije koriste. Takođe u poslovnom okruženju ponekad je lakše da korisnik pristupi nekom veb servisu preko spoljašnjeg naloga, naročito ako je u tom okruženju na određeno vreme i nema potrebe da se zavodi u internu bazu firme koja iznajmljuje njegove usluge, pogotovo ako rešenje kao što je ISAM koje zavodi svaki vid autentifikacije koji prođe ili pokuša da prođe do servisa. S obzirom da je ISAM dobio unapređenje i od verzije ISAM 9.0.4.0 postupak konfiguracije opcije *relying party* koja omogućava da usled federacije ISAM-a sa drugim provajderom identiteta razgraniči uloge u toj istoj federaciji, odnosno ko će da bude provajder identiteta a ko strana koja će da pruža usluge. Postupak konfiguracije nakon nadogradnje je svrstan u par koraka:

- Preduslovi
- *"Relying party"* federacija
- Mapiranje atributa
- Usklađivanje *Facebook Connect* – ISAM
- Otkrivanje federacije *reverse Proxy*-ju

Preduslovi

Pre bilo kakve integracije neophodno je pripremiti ISAM okruženje. Tačnije neophodno je da imamo standardno ISAM okruženje koje podrazumeva:

- Instaliranu verziju ISAM rešenja koja je verzije ISAM 9.0.4.0 ili novije
- Na ISAM okruženju konfigurisan *WebSEAL reverse Proxy* sa osnovnim podešavanjima i
- Aktivan federacioni modul u okviru ISAM okruženja

"Relying party" federacija

Nakon što smo obezbedili sve preduslove za ovu integraciju krenućemo na konfigurisanje federacije odnosno modula u ISAM okruženju koji će nam omogućiti ovu integraciju ISAM rešenja sa *Facebook* platformom. Potrebno je napraviti federaciju koja će imati protokol *OpenID Connect Relying Party*. Takođe je neophodno da kažemo prilikom autorizacije odnosno procesa OpenID Connect protokola kome će se obraćati klijent za autorizaciju odnosno da kažemo da će ISAM sa svojim internim protokolom vršiti autorizaciju. Uz to je za početak neophodno i definisati kakav će povratni zahtev biti kao i na koji način će se mapiranje atributa izvršiti.

Mapiranje atributa

Što se mapiranja atributa tiče generalno za ISAM okruženje, prilikom bilo kakve veze odnosno integracije, mapiranje atributa se vrši uz pomoć takozvanih pravila mapiranja (*mapping rule*). Čemu služe? Pravila mapiranja služe da kažemo ISAM okruženju koje atribute treba da očekuje, odnosno koji atributi sa strane ISAM-ovog skladišta korisnika odgovaraju atributima aplikacije sa kojom se vrši integracija. Recimo u aplikaciji kao što je

Facebook polje „korisničko ime" se vodi kao "*username*" a u ISAM okruženju odnosno njegovom skladištu korisnika isto to polje se zavodi kao "uid". Tako da je neophodno da mi prilikom veze ISAM-a i *Facebook* aplikacije kažemo preko pravila mapiranja da atribut "uid" iz ISAM-a ustvari odgovara atributu "username" iz *Facebook* aplikacije.

Usklađivanje Facebook Connect – ISAM

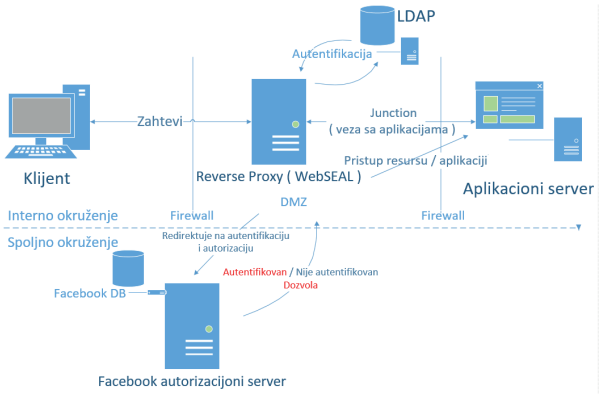
Usklađivanje dva sistema, dve aplikacije, platforme kada pričamo o federaciji, odnosi se na način na koji će ta dva okruženja da se upoznaju, odnosno steknu uzajamno poverenje. Kada pričamo o ISAM rešenju i sa strane samog ISAM-a da bi se steklo uzajamno poverenje sa drugom veb aplikacijom neophodno je da se ispune dva uslova:

- Da ISAM sadrži SSL sertifikate o postojećoj veb aplikaciji ako je zahtevana sigurna veza između ISAM-a i te veb aplikacije i
- Da se federaciji samim tim i ISAM-u proslede takozvani „kredencijali klijenta" koji zapravo predstavljaju identifikaciju klijent aplikacije na internetu.

Otkrivanje federacije reverse Proxy-ju

Nakon što smo završili i imamo do kraja, pravilno konfigurisanu federaciju neophodno je da se takva federacija upozna, odnosno kaže "reverse Proxy-ju" da u nju ima puno poverenje. Nakon tog koraka imamo sigurnu federaciju ISAM-a sa nekom veb aplikacijom u kome će ISAM kao takav pružati dodatnu mogućnost pored zaštite aplikacije i omogućavanja pristupa svojim internim korisnicima, omogućavati i siguran pristup spoljašnjih korisnika putem svojih *Facebook* naloga.

Usled ovako podešenog okruženja, dobili smo jedan siguran i poverljiv sistem zaštite sa mogućnošću proširenja opsega korisnika. U glavnini, proces tog okruženja bi izgledao ovako.



Slika 5. Proces federacije ISAM-a sa Facebook-om

8. ZAKLJUČAK

Ako pričamo o nekom poslovnom okruženju, firme uglavnom žele da veliki deo informacija koje protiču kroz nju budu tajna, samim tim ovakav vid integracije im baš i ne odgovara i uvek gledaju kako bi tako neki pristup učinili internim i zatvorenim. Ali pošto živimo u dinamičnom okruženju i tržište se jako brzo menja i raste kao i to da je zahtevnije i očekuje kvalitetnu uslugu za kratak period, nastala su ovakva okruženja i samo postojanje federacije kao procesa integracije je tu da olakša proširenje i ubrza pristup željenim informacijama i uslugama. Svakako ćemo se složiti da ubacivanje treće strane od poverenja nije najsrećnije rešenje i u velikom broju slučajeva se izbegava ali uslovi kao što su ovi zahtevaju ovakav vid integracije. IBM kao korporacija stoji iza svog proizvoda i garantuje sigurnost i integritet samog SAM proizvoda kao i u spoljnu, proširenu(*federated*) verziju istog. Ovaj vid usluge je pogodan za ovakva okruženja de je potrebno izvršiti kratkoročnu ili trenutnu uslugu. Takođe sa druge strane imamo *Facebook* kao jednu veliku i pouzdanu korporaciju sa preko 2.3 milijarde aktivnih korisnika koja pruža kvalitetnu uslugu na jako zavidnom nivou. Ovakav vid federacije i rešenja bi mogao da ima veliku primenu u nekim internim sistemima u pogledu rasterećivanja sopstvenih sistema, možda čak i širenja firmi i korisnika u različitim delovima sveta. Na taj način bi moglo da se izvrši sigurno spajanje i razmena informacija nevezano od mesta grananja i rasta poslovanja.

LITERATURA

[1] P.Nye. "ISAM Facebook Login with OIDC Relying Party."https://philipnye.com. https://philipnye.com/2018/05/03/isam- facebook-login-with-oidc-relying-party (accessed Mar. 28,2019)

[2] IBM Knowledge Centar. "Federation overview." https://www.ibm.com. https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.6/com.ibm.isam.doc/config/concept/federation_overview.html (accessed Mar. 28,2019)

[3] A.Parecki. "OAuth 2.0." https://oauth.net. https://oauth.net/2/ (accessed Mar. 28,2019)

[4] Jon Harry,Technical Sales Enablement, OpenID Connect Including Advanced Configuration and Access Policies

[5] Wikipedia. "Facebook Platform." https://en.wikipedia.org. https://en.wikipedia.org/wiki/Facebook_Platform (accessed Mar. 28,2019)

[6] Wikipedia. "Facebook Platform#Facebook_Connect." https://en.wikipedia.org. https://en.wikipedia.org/wiki/Facebook_Platform#Facebook_Connect (accessed Mar. 28,2019)

[7] J.Kilani. "Updating Your Privacy Policy for Social Logins." https://www.termsfeed.com. https://www.termsfeed.com/blog/privacy-policy-social-login/ (accessed Mar. 28,2019)