**UNIVERZITET U BANJOJ LUCI**

**ELEKTROTEHNIČKI FAKULTET**

**Rajo Gajić**

**REALIZACIJA SSO SERVERA**

**Diplomski rad**

**Banja Luka, 2017**

**Tema: REALIZACIJA SSO SERVERA**

**Komisija: prof. dr Slavko Marić**

**prof. dr Zoran Đurić**

**mr Ognjen Joldžić**

**kandidat:**

**Rajo Gajić**

UNIVERZITET U BANJOJ LUCI

ELEKTROTEHNIČKI FAKULTET

KATEDRA ZA RAČUNARSKU TEHNIKU

Predmet: INTERNET PROGRAMIRANJE

Tema: REALIZACIJA SSO SERVERA

Zadatak:

Uvod. Autentifikacija i upravljanje identitetima. Autorizacija i kontrola pristupa. SAML. XACML. Dati pregled i analizu postojećih SSO rješenja. Realizovati SSO server, sa osnovnim SSO funkcionalnostima, koji omogućava autentifikaciju i autorizaciju korisnika. Dati uporednu analizu realizovanog rješenja sa postojećim rješenjima.

Mentor: prof. dr Zoran Đurić

Kandidat: Rajo Gajić (22/07)

Banja Luka, 2017

Sadržaj

[1. UVOD 1](#_Toc499388295)

[2. AUTENTIKACIJA 3](#_Toc499388296)

[2.1 Autentifikacija upotrebom lozinke 3](#_Toc499388297)

[2.2 Autentifikacioni faktori 4](#_Toc499388298)

[3. UPRAVLJANJE IDENTITETIMA 5](#_Toc499388299)

[4. SINGLE-SIGN ON (SSO) 7](#_Toc499388300)

[5. AUTORIZACIJA I KONTROLA PRISTUPA 11](#_Toc499388301)

[5.1 Autorizacija 11](#_Toc499388302)

[5.2 Kontrola pristupa 11](#_Toc499388303)

[6. SAML (SECURITY ASSERTION MARKUP LANGUAGE) 13](#_Toc499388304)

[6.1 Principi 13](#_Toc499388305)

[6.2 Kako SAML funkcioniše 13](#_Toc499388306)

[6.2.1 Assertions (tvrdnje) 14](#_Toc499388307)

[6.2.2 Protocols (protokoli) 14](#_Toc499388308)

[6.2.3 Bindings (povezivanja) 15](#_Toc499388309)

[6.2.4 Profiles (profili) 15](#_Toc499388310)

[6.3 SAML 2.0 16](#_Toc499388311)

[7. XACML (EXTENSIBLE ACCESS CONTROL MARKUP LANGUAGE) 17](#_Toc499388312)

[7.1 Konstrukcije najvišeg nivoa: propisi (Policy) i skupovi propisa (PolicySet) 18](#_Toc499388313)

[7.2 Ciljevi (Targets) i pravila (Rules) 18](#_Toc499388314)

[7.3 Atributi (Attributes), vrijednosti atributa (Attribute Values) i funkcije (Functions) 19](#_Toc499388315)

[7.4 Primjer jednog propisa 20](#_Toc499388316)

[8. IZBOR STRATEGIJE ZA REALIZACIJU SSO SERVERA 23](#_Toc499388317)

[8.1 SAML 2.0 23](#_Toc499388318)

[8.1.1 SAML token (Token) vs. SAML tvrdnja (Assertion) 25](#_Toc499388319)

[8.1.2 SAML ograničenja 25](#_Toc499388320)

[8.1.3 Zaobilazno rješenje SAML HTTP POST uvezivanja 26](#_Toc499388321)

[8.2 OAuth 2.0 26](#_Toc499388322)

[8.2.1 OAuth2 nedostaci 28](#_Toc499388323)

[8.3 Rezime – SAML vs. OAuth2 29](#_Toc499388324)

[9. IMPLEMENTACIJA SSO SERVERA 30](#_Toc499388325)

[9.1 Web Browser SSO profil 30](#_Toc499388326)

[9.2 Integracija SSO klijenata sa SSO serverom 34](#_Toc499388327)

[9.2.1 Pozadinski proces prilikom pristupa zaštićenoj stranici na strani SP-a 35](#_Toc499388328)

[10. ZAKLJUČAK 38](#_Toc499388329)

[11. LITERATURA 39](#_Toc499388330)

# UVOD

U današnje vrijeme, IT sistemi se koriste za svakodnevno obavljanje poslova u organizacijama iz raznovrsnih grana industrije. Zavisno od same prirode poslova i procesa koji se obavljaju, takvi sistemi se primjenjuju u manjoj ili većoj mjeri, od čega zavisi i broj tj. raznovrsnost aplikacija koje se pri tome koriste. Uobičajeno je da svaka od tih aplikacija kojoj korisnik ili zaposleni pristupa svakog radnog dana, zahtjeva i provjeru njegovog identiteta, iz sigurnosnih razloga. S obzirom na to da broj tih aplikacija može biti prilično velik, i da svaka od njih zahtijeva identifikaciju, korisnik mora pamtiti veliki broj pristupnih podataka odnosno lozinki za svaku od njih, što često predstavlja problem i povećava broj poziva prema korisničkoj podršci. To dovodi do nepotrebnog gubitka vremena predviđenog za konkretan rad, a uz to predstavlja i dodatni posao za tehničko osoblje kao i otežano održavanje korisničkih naloga, s obzirom na njihov veliki broj.

Gore navedeni problem, doveo je do razvoja procesa za autentikaciju korisnika upotrebom jednokratnog prijavljivanja, poznatijeg pod nazivom *Single sign-on (SSO).* Ovaj proces omogućava korisniku da se samo jednim unošenjem korisničkog imena i lozinke prijavi u više aplikacija. Najveće prednosti upotrebe ovakvog procesa su:

* Jednostavan i brz proces prijave korisnika
* Olakšano održavanje korisničkih naloga
* Povećana sigurnost sistema
* Istorija pristupa aplikacijama

Bitno je napomenuti da se SSO proces uveliko koristi i u svakodnevnom radu korisnika na internetu, s obzirom na činjenicu da većina vodećih IT kompanija poput Google-a, Facebook-a i ostalih, korisnicima nude različite aplikacije za određenu namjenu, zavisno od njihovih interesovanja. Uobičajeno je da korisnik može pristupiti svakoj od tih nezavisnih aplikacija, koje su pod vlasništvom jedne kompanije, upotrebom istih pristupnih podataka tj. korišćenjem jednog istog naloga. Pored toga, takvi nalozi se mogu koristiti i za pristup aplikacijama drugih kompanija koje koriste njihov SSO servis. Često je moguće vidjeti opciju prijavljivanja na određenu web aplikaciju upotrebom postojećeg Facebook ili Google naloga.

U narednom poglavlju dat je detaljniji opis SSO procesa autentikacije kao i odgovarajućih sistema koji učestvuju u njemu. Osnovni pod procesi SSO procesa, kao što su autentikacija, upravljanje identitetima, te autorizacija i kontrola pristupa, koji grubo rečeno služe za utvrđivanje identiteta korisnika i njegovih dozvola na sistemu, opisani su u poglavljima 3, 4 i 5, respektivno. U poglavlju 6 i 7 izvršena je analiza SAML i XACML standarda koji se koriste pri razmijeni autentikacionih i autorizacionih poruka između sistema uključenih u SSO proces. Na kraju, u poglavljima 8, 9 i 10 dato je objašnjenje izbora strategije za realizaciju SSO servera te sami detalji njegove implementacije, koja je praktični dio ovog rada, kao i uporedna analiza realizovanog rješenja sa postojećim rješenjima predstavljenim i analiziranim u poglavlju ?.

# AUTENTIKACIJA

Autentikacija je proces određivanja identiteta subjekta, najčešće fizičke osobe, upotrebom pristupnih podataka na osnovu kojih se može utvrditi da je subjekat upravo taj za koga se predstavlja. Pri tom procesu pristupni podaci se upoređuju sa podacima u bazi ili nekom drugom izvoru liste podataka registrovanih tj. ovlašćenih korisnika. Ako se oni poklapaju, proces autentikacije je uspješno završen i korisnik dobija ovlašćenje za pristup sistemu.

Autentikacija može biti sprovedena upotrebom pristupnih podataka, SSO sistema, biometrijski, digitalnim certifikatima i javnim ključevima.

Autentikacija korisnika je ključna za osiguravanje odgovarajućih ovlašćenja i prava pristupa sistemima i uslugama, naročito od kada je sve učestalija krađa podataka i sve su veće prijetnje sigurnosti informacija. Iako autentikacija ne može u potpunosti spriječiti krađu informacija i identiteta, takve resurse moguće je zaštititi upotrebom jedne ili više autentikacijskih metoda.

## Autentikacija upotrebom lozinke

U privatnim i javnim računarskim mrežama (uključujući internet), autentikacija se najčešće realizuje upotrebom korisničkog imena i lozinke. Pretpostavlja se da je poznavanje pristupnih podataka dovoljna garancija da je korisnik ispravan, tj. onaj za koga se prestavlja. Svaki korisnik se pri prvoj upotrebi sistema registruje (ili ga je već neko registrovao, npr. sistem administrator) upotrebom korisničkog imena i lozinke, bilo predodređene ili po svom izboru. Međutim, autentikacija na osnovu korisničkog imena i lozinke se ne smatra dovoljno sigurnom i pouzdanom za bilo koji sistem koji sadrži osjetljive podatke.

Korisnička imena su često kombinacija imena i prezimena osobe, zbog čega ih je lako pogoditi. Pored toga, ljudi često prave i slabe lozinke, ukoliko se ne postave pravila za njihovo kreiranje. Međutim, čak i jake lozinke mogu biti ukradene, slučajno otkrivene ili zaboravljene. Iz tog razloga, internet poslovanje i mnoge druge transakcije zahtijevaju strože procese i metode autentikacije.

Nedostaci autentikacije na osnovu lozinke mogu se nadoknaditi upotrebom kompleksnijih korisničkih imena koja nije lako pogoditi te definisanjem pravila za kreiranje sigurnije lozinke, kao što su minimalna dužina te kombinovanje velikih i malih slova sa brojevima i simbolima.

Uprkos tome, sistemi koji koriste autentikaciju na osnovu lozinke i generalno autentikaciju na osnovu „nečega što znamo“ su mnogo ranjiviji nego oni koji koriste nekoliko nezavisnih metoda autentikacije.

Autentikacioni faktor odnosno metod predstavlja način na koji se vrši provjera identifikacije korisnika. Tri najčešće kategorije su opisane kao „nešto što znamo“ (faktor znanja), „nešto što posjedujemo“ (faktor posjedovanja) i „nešto što jesmo“ (faktor nasljeđivanja).

## Autentikacioni faktori

* Faktori znanja – kategorija identifikatora koja sa sastoji od informacija koje korisnik zna, kao što su lični identifikacioni broj (PIN-*Personal Identification Number*), korisničko ime, lozinka ili odgovor na tajno pitanje.
* Faktori posjedovanja – kategorija identifikatora koja se zasniva na predmetima koje korisnik ima uz sebe, najčešće u obliku fizičkog uređaja kao što je sigurnosni token ili mobilni telefon sa instaliranom aplikacijom koja generiše token.
* Faktori nasljeđivanja – kategorija identifikatora koja se sastoji od elemenata koji su svojstveni pojedincu, u obliku biometrijskih podataka kao što je npr. otisak prsta, mrežnjača oka itd.

Lokacija korisnika i trenutno vrijeme su nešto što se smatra četvrtim i petim faktorom autentikacije. Rasprostranjenost pametnih telefona olakšava primjenjivanje autentikacije korisnika upotrebom više faktora. Većina pametnih telefona opremljena je GPS-om, tj. sistemom za lociranje pomoću satelita, omogućavajući time relativno pouzdanu provjeru lokacije sa koje se korisnik prijavljuje. Manje pouzdane mjere su upotreba MAC adrese pristupne tačke ili provjera fizičke prisutnosti upotrebom kartica i ostalih elemenata autentikacionog faktora posjedovanja.

Upotreba više faktora autentikacije postala je uobičajena praksa za prijavljivanje i izvršavanje transakcija u okviru sistema koji zahtijevaju visok nivo sigurnosti. Šta više, dvostepena autentikacija postaje standard za upotrebu u okviru uobičajenih sistema, dok se autentikacija sa tri ili više faktora koristi u sistemima koji imaju izuzetno visok stepen sigurnosti. Na ovaj način sigurnost se znatno uvećava, s obzirom na to da je mala vjerovatnoća da će napadač doći u posijed svim faktorima koji su potrebni za autentikaciju.

# UPRAVLJANJE IDENTITETIMA

Upravljanje identitetima je administrativna oblast koja se bavi identifikovanjem subjekata u sistemu i kontrolisanjem njihovog pristupa resursima u okviru njega. Prava pristupa resursima i određenim funkcionalnostima sistema definišu se povezivanjem standardnih, unaprijed definisanih korisničkih prava sa utvrđenim identitetom subjekta.

Na najnižem nivou, upravljanje identitetima podrazumijeva definisanje onoga šta korisnik može raditi na mreži sa specifičnim uređajima i pod kojim okolnostima. Danas, mnogi sigurnosni proizvodi imaju naglasak na upravljanju mobilnog pristupa korporativnim sistemima. U enterprise okruženju, upravljanje identitetima se koristi zbog poboljšanja sigurnosti i produktivnosti, pri čemu se smanjuju troškovi i suvišan napor.

Upravljanje identitetima je postalo veoma bitno pitanje u IT svijetu. Kako su web aplikacije vremenom rasle kako bi podržale mnoštvo poslovnih procesa, povećao se i broj korisnika, grupa i uloga (*rola*) kojima treba upravljati. Kako se povećava broj sistema koji se uvode, povećava se i napor za sistem administratore i timove za podršku.

Što se tiče upravljanja identitetima (nalozima i korisničkim pristupom), postoje mnogi izazovi za pravilno upravljanje. Neki od njih uključuju kreiranje naloga, kao i njihovo održavanje i uklanjanje. Drugi izazov je, koji je najbolji način da se obezbijedi autentikacija za korisnike. To može obuhvatati pravila vezana za lozinke i/ili biometriju te odgovor na pitanje kako potvrditi korisničke podatke na način da se zaštiti kompanija, a istovremeno umanji napor potreban kako bi se korisnik autentikovao u okviru više sistema.

Odgovor odnosno rješenje na prethodno navedene izazove nalazi se u upotrebi SSO-a i sistema za upravljanje identitetima. Odgovarajuća implementacija takvog sistema može značajno umanjiti cjelokupan administrativni posao neophodan pri upravljanju korisničkim informacijama u centralizovanom skladištu. Neki od problema koje ovakav sistem može riješiti su:

* Prevelik broj timova uključen u administraciju korisnika
* Kreiranje naloga od strane zaposlenih koji nemaju odgovarajuća prava pristupa
* Nepostojanje standarda pri kreiranju korisničkih naloga, što dovodi do toga da jedan korisnik ima više različitih naloga sa različitim dozvolama u okviru istog sistema
* Spor odziv pri održavanju naloga, zbog postojanja birokratije u održavanju različitih sistema i koordinisanja različitih pristupnih pravila između nekoliko grupa
* Suvišne ili netačne informacije koje djelimično identifikuju direktorije i identitete

Aplikacije mogu koristiti SSO proces kako bi obezbijedile korisnicima jednostavan i brz pristup sadržaju koji se čuva i uređuje na različitim vrstama sistema. To se postiže tako što se omogućava višestruka prijava upotrebom istog korisničkog imena i lozinke. Više detalja o samom SSO procesu i načinu funkcionisanja nalazi se u narednom poglavlju.

Iz sigurnosnih razloga, alati za upravljanje identitetima trebalo bi da se izvršavaju kao aplikacija na posebnom mrežnom uređaju ili serveru, bilo lokalno ili *cloud*. Jezgro sistema za upravljanje identitetima čine pravila koja definišu koji uređaji i korisnici su dozvoljeni na mreži i šta korisnik može postići, zavisno od tipa njegovog uređaja, lokacije i drugih faktora. Velika prednost je i izvještavanje o aktivnostima sistema koje proizvodi revizijski dnevnik u koji se bilježe sve specifične aktivnosti koje su izvršene.

# SINGLE-SIGN ON (SSO)

SSO je metodologija koja obezbjeđuje jednu akciju za autentikaciju i autorizaciju korisnika, čime im se omogućuje pristup svim računarima i sistemima na koje imaju prava, bez potrebe da se identifikuju nekoliko puta. Nudeći tu mogućnost, SSO značajno umanjuje ljudsku grešku koja je najčešći uzrok pada sistema. Moglo bi se reći da je najznačajnija stvar posjedovanja centralizovanog sistema, postojanje centralnog skladišta u kom se čuvaju svi korisnički pristupni podaci i dozvole, čime se rješava problem njihovog postojanja u okviru svake od aplikacija pojedinačno. Povezivanje više različitih aplikacija upotrebom integrisanog sistema, omogućava i internim i eksternim korisnicima da koriste isto korisničko ime i lozinku za prijavu na svaku od njih.

Na **Slici 4.1** prikazan je scenario prijave korisnika na dvije različite aplikacije, bez postojanja SSO servera.

domen1.com

**Skladište kolačića preglednika**

domen2.com



Unos pristupnih podataka,

identifikovanje korisnika

**BEZ SSO SERVERA**

Unos pristupnih podataka,

identifikovanje korisnika

Odlazi na

Odlazi na

**Korisnik**

Čuva kolačić

Čuva kolačić

Slika 4.1 – Rješenje bez SSO servera

Kao što je moguće vidjeti na prethodnoj slici, korisnik nakon odlaska na svaki od domena mora da se prijavljuje pojedinačno. Nakon uspješne prijave, u skladište kolačića njegovog preglednika čuva se kolačić koji služi kao identifikator sesije u okviru koje je korisnik autentikovan.

Očigledno rješenje ovog problema je dijeljenje informacija o sesijama između različitih domena, predstavljeno na **Slici 4.2**. Međutim, zbog sigurnosnih razloga, preglednik primjenjuje pravilo poznato kao *same-origin-policy* – pravilo istog porijekla. Ovo pravilo kaže da kolačićima (*cookies*) i ostalim podacima lokalne pohrane podataka, može pristupiti samo onaj ko ih je napravio, tj domen koji je napravio zahtjev za čuvanje tih podataka. Drugim riječima, domen X ne može pristupiti kolačićima kreiranim od strane domena Y i obrnuto. To je ono što SSO rješava: dijeljenje sesijskih informacija između različitih domena.

domen1.com

**Skladište kolačića preglednika**

domen2.com



Unos pristupnih podataka,

identifikovanje korisnika

**PRAVILO ISTOG PORIJEKLA**

**SPRIJEČAVA OVO**

Koristi kolačić domena1,

Identifikuje korisnika

Odlazi na

Odlazi na

**Korisnik**

Čuva kolačić

Čita kolačić domena1

Slika 4.4.1 - Pravilo istog porijekla

Različiti SSO protokoli dijele sesijske podatke na različite načine, ali osnovni princip je isti – postoji centralni domen preko kog se vrši autentikacija, nakon čega se sesija dijeli sa ostalim domenima na neki način. Npr. centralni domen generiše potpisani SAML token (koji može biti šifrovan). Taj token se dalje može proslijediti klijentu i može se koristiti od strane autentikacijskog domena kao i od strane ostalih domena. Token može biti proslijeđen izvornom domenu putem redirekcije, pri čemu on sadrži sve informacije potrebne za identifikaciju korisnika u okviru domena koji je zahtijevao autentikaciju. S obzirom na to da je token potpisan, ne može biti izmijenjen od strane klijenta ni na koji način. Ovaj scenario prikazan je na **slici 4.3**.

domen1.com

**Skladište kolačića preglednika**

domen2.com



**UPOTREBA DOMENA ZA CENTRALNU AUTENTIKACIJU**

Odlazi na

**Korisnik**

**Autentikacioni server**

(domen3.com)

Odlazi na

Preusmjeravanje

Preusmjeravanje

Slika 4.3 - Upotreba centralnog autentikacionog domena

Svaki put kada korisnik posjeti domen koji zahtjeva autentikaciju, preusmjeren je na autentikacijski domen. S obzirom na to da je korisnik već prijavljen pod tim domenom, može odmah biti preusmjeren na izvorni domen uz neophodni autentikacijski token. Uobičajeni scenario prijave korisnika upotrebom SSO servera, prikazan je na **slici 4.4**.

domen1.com

**Skladište kolačića preglednika**

domen2.com



Preusmijerava na

**UOBIČAJENI SSO**

Koristi token

za autentikaciju

Odlazi na

Odlazi na

**Korisnik**

Čuva kolačić

za domen1

**Autentikacioni server**

(domen3.com)

Čuva kolačić

za domen2

Koristi token

za autentikaciju

Šalje token i preusmijerava

Čuva kolačić

Preusmijerava na

Korisnik se identifikuje ili je kolačić dostupan

Šalje token i preusmijerava

Slika 4.2.4 - Uobičajeni SSO scenario

U uobičajenoj konfiguraciji SSO-a koja je navedena u gore prikazanom scenariju, korisnik prvo odlazi na domen1 na kom još uvijek nije prijavljen, zbog čega se vrši preusmjeravanje na autentikacioni domen odnosno SSO server. Ukoliko korisnik nije bio prijavljen u okviru njega (sesijski kolačić nije dostupan), korisnik se prvo autentikuje na centralnom autentikacionom serveru gdje dobija svoju sesiju i odgovarajući kolačić. Nakon toga, on se preusmjerava nazad na izvorni domen, zajedno sa autentikacijskim tokenom, na osnovu kog se vrši autentikaciju i čuvanje kolačića u okviru domena1, s obizirom na to da token sadrži sve informacije potrebne za to. Sada, ukoliko korisnik posjeti domen2 u okviru kog još uvijek nije prijavljen, ponovo se vrši preusmjeravanje na SSO server. Međutim, kako je korisnik ovaj put već prijavljen u okviru njega, odnosno posjeduje sesijski kolačić koji drži informaciju o sesiji u okviru koje je on autentikovan na SSO server, nije potrebna ponovna identifikacija korisnika, već se on automatski preusmjerava na izvorni domen zajedno sa tokenom. Autentikacijski domen ponovo sadrži informacije neophodne za autentikaciju korisnika, ali ovaj put u okviru domena2, tako da se token koristi za autentikaciju i u okviru njega.

Single sign-on (SSO) je oblik tehnologije koji olakšava proces autentikacije kako za korisnike tako i za IT administratore. Ukoliko se koristi SSO sistem, dovoljno je da korisnik samo jednom unese korisničko ime i lozinku kako bi dobio pristup na vise aplikacija. Korisnicima se posle registracije dodjeljuju prava pristupa određenim aplikacijama, nakon čega su u stanju da pristupe tim aplikacijama kada unesu svoje pristupne podatke, što eliminiše višestruke unose i prijavu. SSO takođe smanjuje vrijeme i cijenu uređivanja velikog broja lozinki za IT osoblje.

SSO sistemi unaprijeđuju sigurnost time što se cjelokupna autentikacija izvršava u okviru posebnog servera za tu namjenu. Svi autentikacioni podaci moraju prvo proći kroz poseban server za SSO, koji zatim dalje proslijeđuje određene autentikacione informacije koje posjeduje za datog korisnika. Ovakav način centralizovanog sistema za autentikaciju će vjerovatno prije odoljeti napadima i zlonamjernom pristupu nego obični autentikacioni sistem. Dodatno, SSO sistemi obično obezbjeđuju bolju zaštitu osjetljivog materijala, s obzirom na to da su najčešće zaštićeni firewall-om.

SSO je takođe koristan za dokumentovanje pristupa i nadzor korisničkih naloga – npr. čišćenje neaktivnih korisničkih naloga zaposlenih i praćenje aktivnosti korisnika.

# AUTORIZACIJA I KONTROLA PRISTUPA

## Autorizacija

Autorizacija je proces dodjeljivanja dozvola nekome da uradi ili posjeduje nešto. U višekorisničkim računarskim sistemima, sistem administrator definiše koji korisnici imaju pristup sistemu i koje privilegije posjeduju u okviru njega (kao što su pristup određenim direktorijima, trajanje i vrijeme pristupa, količina skladišnog prostora itd.). Nakon prijave u računarski operativni sistem ili aplikaciju, identifikuje se kojim resursima korisnik može pristupiti tokom sesije. Prema tome, autorizaciju je moguće posmatrati i kao početna podešavanja dozvola definisana od strane sistem administratora, i kao provjeru dozvola koje se dodjeljuju korisniku nakon što je dobio pristup sistemu.

Autentikacija provjerava identitet korisnika i omogućava autorizaciju. Autorizacijska pravila diktiraju šta korisnik ima pravo da izvršava. Npr. bilo koja mušterija banke može kreirati svoj nalog kako bi pristupila online sistemu banke, ali autorizaciona pravila banke moraju da se pobrinu da samo taj korisnik ima pravo pristupa svom ličnom nalogu nakon što se potvrdi njegov identitet. Jednostavno rečeno, autorizacija je proces sprovođenja pravila: određivanje kojim vrstama ili funkcionalnostima aktivnosti, resursa ili usluga korisnik ima pristup. Uobičajeno, autorizacija se dešava u okviru procesa autentikacije. Nakon što se korisnik autentikuje, mogu mu se odobriti različiti tipovi pristupa ili aktivnosti.

Autorizacija može biti primijenjena u mnogo složenijem obliku nego što je to npr. pravo pristupa web sajtu ili internoj mreži kompanije. Korisnički nalog može biti uključen u grupu naloga koji dijele zajednička autorizacijska pravila. Npr. recimo da postoji baza podataka koja sadrži transakcije kupaca ali i njihove lične podatke i podatke o kreditnoj kartici. Trgovac bi mogao kreirati autorizacijsko pravilo za ovu bazu podataka, tako da dozvoli grupi marketinga pristup svim kupovinama mušterija ali pri tome spriječavajući pristup ličnim podacima kupaca i podacima njihovih kreditnih kartica, kako bi marketinška grupa mogla identifikovati popularne proizvode u cilju njihovog promovisanja ili rasprodaje.

Korisnici implicitno kreiraju autorizacijska pravila kada koriste socijalne medije: Facebook, LinkedIn ili Twiter autentikuju stotine miliona korisnika, ali u izvjesnoj mjeri korisnik može sam odrediti pravila da li i u koliko mjeri ostvaruje kontakt sa drugim korisnicima. Isti je slučaj sa dijeljenjem datoteka, video klipova ili fotografija na sajtovima kao što su Google Docs, Dropbox, Instagram, Pinterest ili čak i sa pravljenjem dijeljenog direktorijuma na laptopu.

## Kontrola pristupa

Dok autorizacijska pravila definišu čemu određeni korisnik ili grupa korisnika može pristupiti, kontrola pristupa, predstavlja metode koje se koriste za sprovođenje tih pravila. Kontrola pristupa reguliše odluke i procese utvrđivanja, dokumentovanja i upravljanja resursima (korisnicima, uređajima ili procesima) kojima treba dobiti pristup, kao i subjektima kojima bi on trebao biti omogućen. Kontrola pristupa takođe reguliše metode i uslove pod kojima je dozvoljen ili onemogućen pristup zahtijevanim resursima. Neki od primjera:

* Kroz podešavanja Facebook-a – Ko može vidjeti stvari određenog profila ? Ko može kontaktirati taj profil ? Ko može pronaći profil ? – Nekim korisnicima ili javnosti dozvoljava se ili onemogućuje pristup onome što određeni korisnik postavlja na svoj Facebook profil.
* Podešavanja Google Docs-a omogućavaju postavljanje dozvola za izmjenu ili dijeljenje dokumenata koji se zajednički koriste od strane više osoba.
* Flickr podešavanja dozvoljavaju kreiranje ili dijeljenje albuma ili slike sa porodicom, prijateljima ili sa javnošću.

Ispravno podešavanje prava pristupa je ključna komponenta zaštite informacija od neodobrenog pristupa i zaštite računarskih sistema od zloupotrebe. Međutim, podešavanje tih prava pristupa nije jednostavan posao.

# SAML (SECURITY ASSERTION MARKUP LANGUAGE)

SAML je otvoreni, standardizovani format poruka, zasnovan na XML-u koji služi za razmjenu autentikacionih i autorizacionih podataka. Komunikacija se najčešće vrši između provajdera identiteta i servisnog provajdera, u okviru single sign-on (SSO) procesa putem internet preglednika, što i jeste jedna od najvažnijih uloga za koju se SAML koristi. Razvijen je od strane OASIS-a[[1]](#footnote-1) i datira još iz 2001. godine, s tim da se konstantno vrše nadogradnje i unapređenja.

## Principi

Postoje tri različite uloge u scenarijima koje propisuje SAML specifikacija:

* *Principal* (korisnik) - subjekat koji može biti autentikovan u okviru određenog sigurnosnog domena
* *Identity Provider* skr. IdP (provajder identiteta) - sistem koji služi za dodavanje, održavanje i upravljanje informacijama o identitetu subjekta, kao i za njihovo izdavanje u obliku SAML tvrdnji koje su opisane u tački 6.2.1.
* *Service Provider* skr. SP (servis provajder)- sistem odnosno servis čijim resursima korisnik želi pristupiti, i koji obavlja komunikaciju sa provajderom identiteta u cilju sprovođenja kontrole pristupa

Uobičajeni tok dešavanja u tim scenarijima počinje tako što korisnik traži pristup resursu ili određenoj usluzi na strani servis provajdera. Servis provajder zatim od pravajdera identiteta zahtjeva i dobavlja tvrdnje o identitetu korisnika, te na osnovu njih vrši odluke o pravima pristupa zahtijevanim resursima i uslugama.

Provajder identiteta, prije nego što dostavi tvrdnju o identitetu korisnika servis provajderu, može tražiti neke dodatne informacije od korisnika, kao što su korisničko ime i lozinka, kako bi utvrdio njegov identitet. SAML specifikuje tvrdnje izmedju tri strane, naročito poruke kojim se tvrdi identitet korisnika od strane provajdera identiteta prema servis provajderu. Po SAML specifikaciji, jedan provajder identiteta može slati tvrdnje različitim servis provajderima. Slično, jedan servis provajder može se oslanjati i vjerovati tvrdnjama dobijenim od strane više nezavisnih provajdera identiteta.

SAML ne definiše način na koji će se korisnik autentikovati na strani provajdera identiteta. Mogu se koristiti korisničko ime i lozinka ili neki drugi oblik autentikacije, uključujući autentikaciju u više koraka (*multi factor*).

## Kako SAML funkcioniše

U suštini, SAML nije ništa više nego niz XML baziranih poruka koje daju informaciju o tome da li je korisnik autentikovan, kakva prava pristupa i uloge posjeduje, te na koji način može koristiti podatke i resurse na osnovu toga. Kompatibilan je sa HTTP, SMTP, FTP i SOAP protokolima, uz niz ostalih protokola i tehnologija.

Glavne komponente SAML specifikacije su:

* *Assertions* (tvrdnje)
* *Protocols* (protokoli)
* *Bindings* (povezivanja/uvezivanja)
* *Profiles* (profili)

### Assertions (tvrdnje)

SAML tvrdnja predstavlja skup sigurnosnih informacija dobijenih od strane provajdera identiteta. Primjer koji prikazuje strukturu SAML tvrdnje:

<saml:Assertion ...>

<saml:Issuer>...</saml:Issuer>

<saml:Subject>...</saml:Subject>

<saml:Conditions>...</saml:Conditions>

<saml:AuthnStatement>...</saml:AuthnStatement>

<saml:AttributeStatement>...</saml:AttributeStatement>

<saml:AuthorizationDecisionStatement>...

</saml:AuthorizationDecisionStatement>

</saml:Assertion>

SAML tvrdnje se obično prenose od strane provajdera identiteta prema servis provajderu. Tvrdnje sadrže izjave (*statements*) koje servis provajder koristi kako bi donio odluku o pravima pristupa korisnika, nakon što on uputi zahtjev za pristup određenom resursu ili usluzi. Postoje tri vrste izjava koje SAML prenosi:

1. ***Authentication statements* (autentikacione izjave)** – govore servis provajderu da se korisnik autentikovao na strani provajdera identiteta u određeno vrijeme i upotrebom određene metode za autentikaciju
2. ***Attribute statements* (atributske izjave) –** govore koji specifični atributi su vezani za subjekat odnosno korisnika. Atribut predstavlja jednostavan par podataka, predstavljen u obliku „naziv-vrijednost“. Strana koja konzumira te poruke koristi atribute kako bi donijela odluke o dozvolama i pravima pristupa.
3. ***Authorization decision statements* (autorizacijske odluke) –** govore da li korisnik ima dozvolu da izvrši određenu akciju nad resursom. Izražavanje autorizacionih odluka je nešto gdje je SAML sa namjerom ograničen. Za naprednije slučajeve upotrebe preporučuje se korištenje XACML-a, detaljnije obrađenog u glavi 7.

### Protocols (protokoli)

SAML protokol opisuje način na koji se određeni SAML elementi (uključujući i tvrdnje) pakuju unutar SAML zahtjeva i odgovora, i definiše pravila kojih se SAML učesnici moraju pridržavati prilikom kreiranja ili konzumiranja istih. Najvećim dijelom, SAML protokol je jednostavan protokol koji se zasniva na slanju zahtjeva i primanju odgovora.

Najbitniji tip zahtjeva SAML protokola se naziva *query* (upit). Servis provajder direktno šalje upit provajderu identiteta putem sigurnog kanala. U skladu sa tri tipa izjava, postoje tri tipa SAML upita:

1. Autentikacijski upit
2. Atributski upit
3. Upit autorizacijske odluke

Među navedenim, atributski upit je možda najvažniji. Rezultat takvog upita je SAML odgovor koji sadrži tvrdnju koja se sastoji od gore navedenih atributskih izjava.

### Bindings (povezivanja/uvezivanja)

SAML povezivanje je mapiranje SAML poruka u standardne formate poruka i komunikacione protokole. Npr, SAML SOAP povezivanje specifikuje na koji način se SAML poruka enkapsulira u SOAP poruku, koja je sama po sebi vezana za HTTP poruku.

SAML 1.1 definiše samo jedno povezivanje – SAML SOAP, dok SAML 2.0 sadrži potpuno novu specifikaciju povezivanja koja definiše sledeće standarde:

* *SAML SOAP Binding (based on SOAP 1.1)*
* *Reverse SOAP (PAOS) Binding*
* *HTTP Redirect (GET) Binding*
* *HTTP POST Binding*
* *HTTP Artifact Binding*
* *SAML URI Binding*

Za *Web Browser SSO* profil, koji je detaljnije obrađen kasnije, najčešće se koriste *HTTP Redirect Binding* i *HTTP POST Binding*. Npr, servis provajder može koristiti HTTP redirekciju kako bi poslao zahtjev, dok provajder identiteta koristi HTTP POST metodu za vraćanje odgovora.

### Profiles (profili)

SAML profil detaljno opisuje kako treba da se kombinuju tvrdnje, protokoli i povezivanja za određeni slučaj upotrebe. Najvažniji SAML profil je *Web Browser SSO* profil, detaljno opisan u paragrafu 9.1.

# XACML (EXTENSIBLE ACCESS CONTROL MARKUP LANGUAGE)

XACML (eXtensible Access Control Markup Language) je standard koji definiše jezik zasnovan na XML-u, dizajniran za iskazivanje sigurnosnih propisa i prava pristupa podacima u okviru web servisa i poslovnih sigurnosnih aplikacija. Pored samog jezika, definiše artitekturu kao i proces obrade zahtjeva za pristup, u skladu sa pravilima definisanim unutar propisa. Odobren od strane OASIS-a u Februaru 2003. godine, XACML je razvijen s ciljem uspostavljanja zajedničke terminologije i kompatibilnosti između različitih implementacija sistema za kontrolu pristupa. Za XACML se nekada koristi i naziv XACL (eXtensible Access Control Language).

To je prvenstveno sistem koji vrši kontrolu pristupa na osnovu atributa. Atributi, koji se odnose na entitete sistema bilo u obliku korisnika, resursa, akcije ili okruženja, koriste se za donošenje odluka o tome da li bi korisnik trebao, na određeni način, dobiti pristup željenom resursu ili ne. Pored toga, XACML podržava i kontrolu pristupa na osnovu uloga, što znači da se odluke o pristupu korisnika određenom reursu donose na osnovu uloga koje su mu dodijeljene, i koje sa sobom donose određene dozvole.

Ukoliko su odluke o pristupu enkapsulirane u okviru klijentske aplikacije, te dođe do promjene propisa i regulativa, veoma je teško ažurirati kriterijume koji se koriste za njihovo donošenje. Iz tog razloga, XACML model preporučuje izdvajanje pristupnih odluka van mijesta gdje se one koriste, što olakšava njihovo ažuriranje i omogućuje momentalnu primjenu na svim mjestima upotrebe.

## Arhitektura

Arhitektura XACML-a i primjer odvijanja procesa autorizacije prikazani su na Slici 7.1. Pojmovi koji se koriste pri opisu ovakvih procesa su sledeći:

* PIP (Policy Administration Point) – tačka upravljanja propisima je tačka koja upravlja propisima vezanim za autorizaciju, odnosno dodijelu prava pristupa
* PDP (Policy Decision Point) - tačka donošenja odluka je tačka koja prije izdavanja odluka o pristupu, procijenjuje zahtijev za pristup na osnovu autorizacionih propisa
* PEP (Policy Enforcement Point) - tačka izvršenja propisa je tačka koja presreće zahtjev korisnika za pristupu resursu, izdaje PDP-u zahtjev za donošenje odluke kako bi se utvrdilo da li je korisniku pristup odobren ili ne, a zatim postupa po toj odluci
* PIP (Policy Information Point) – informativna tačka je tačka koja služi kao izvor informacija o vrijednostim atributa nekog entiteta u okviru sistemu (npr. korisnik, resurs, akcija, okruženje)
* PRP (Policy Retrieval Point) - tačka pribavljanja propisa je tačka u kojoj su smješteni XACML propisi vezani za autorizaciju pristupa, najčešće baza ili sistem datoteka



**PEP**

**PDP**

**PAP**

**PIP**

1.Učitaj resurs

2.Da li korisnik ima pristup resursu?

3. Procijena zahtijeva na osnovu propisa

Upravljanje

propisima

3.a..Pribavljanje

dodatnih atributa

4.Dozvola, korisnik

ima pristup resursu

5.Učitaj resurs

**PAP**

Pribavljanje

propisa

Slika .

Odvijanje procesa autorizacije opisano je narednim koracima:

1. Korisnik šalje zahtijev za pristup resursu, koji zatim biva presretnut od strane PEP-a odnosno tačke za izvršenje propisa
2. PEP taj zahtijev konvertuje u XACML zahtjev za autorizaciju i proslijeđuje ga PDP-u, odnosno tački za donošenje odluka
3. PDP na osnovu podešenih propisa procijenjuje zahtijev. Propisi se dobavljaju pomoću tačke za pribavljanje propisa tj PRP-a, dok se za upravljanje njima koristi PAP – tačka za upravljanje propisima.
   1. Ukoliko je potrebno, PDP takođe od informativnih tačaka (PIP) dobavlja vrijednosti atributa koji se odnose na entitete sistema
4. PDP donosi odluku o pristupu (dozvoli / odbij / nije primijenjivo / neodređeno) i vraća je nazad tački za izvršenje propisa – PEP
5. PEP korisniku dozvoljava ili odbija pristup, zavisno od prethodno dobijene odluke

# IZBOR STRATEGIJE ZA REALIZACIJU SSO SERVERA

Vjerovatno ste se već prijavljivali u aplikaciju (mobilnu ili web) klikom na dugme „Prijavi me upotrebom Facebook-a“. Ako koristite Instagram, Spotify ili Pinterest znate o čemu se radi.

Kao korisnik, ne interesuje vas na koji način funkcioniše SSO. Sve što želite je koristiti aplikaciju i imati uglađeno iskustvo, uz što manje pamćenje korisničkih imena i lozinki.

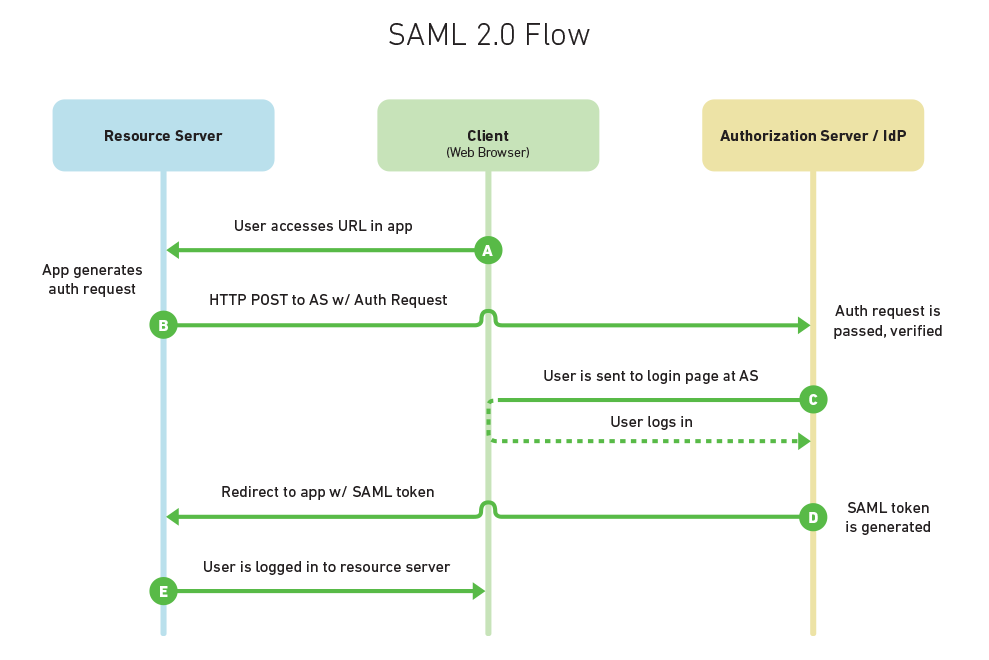
Kako bi se korisniku omogućilo takvo iskustvo, potrebno je implementirati SSO rješenje. Postoji mnogo strategija za implementaciju SSO-a, ali ćemo analizirati i porediti dvije najpopularnije – SAML i OAuth2.

## SAML 2.0

Prvo ćemo baciti pogled na SAML 2.0 koji je skup otvorenih standarda, među kojima je jedan posebno namijenjen i dizajniran za SSO.

SAML 2.0 specifikacija (nadalje SAML) obezbjeđuje „Web Browser SSO Profile“ koji opisuje kako se single-sign-on može postići za web aplikacije. Postoje tri ključna igrača u SAML-u:

* Davalac usluga (Service Provider - SP) – web server kome pokušavamo pristupiti
* Klijent (Client) – način na koji korisnik međudjeluje sa davaocem usluga, kao što je npr. web aplikacija koja je učitana u okviru web preglednika korisnika
* Dobavljač identiteta (Identity Provider - IdP) – server koji posjeduje identitet i pristupne podatke korisnika, tj. potvrđuje identitet korisnika.



Slika 8.1 - Najčešći scenario upotrebe SAML-a

Primjer jednog slučaja upotrebe koji opisuje gornji dijagram:

* A – korisnik otvara web preglednik i posjećuje MyPhotos.com na kome se nalaze sve njegove slike. MyPhotos.com ne može sam vršiti autentifikaciju korisnika.
* B – kako bi autentifikovao korisnika, MyPhotos.com pravi SAML autentifikacijski zahtjev (SAML Authrequest), potpisuje ga, eventualno ga šifruje, a zatim kodira. (šifrovati znači sakriti sadržaj, dok kodirati znači obezbijediti njegovu upotrebo s ciljem izbjegavanja gubitka informacija ili grešaka u prenosu) Nakon toga, preusmjerava web preglednik korisnika na dobavljač identiteta (IdP) s ciljem autentifikacije. IdP prima zahtjev, dekodira ga, koliko je potrebno dešifruje, te provjerava potpis.
* C – Ukoliko je autentifikacijski zahtjev ispravan, IdP će korisniku prikazati stranicu za prijavu na kojoj može unijeti svoje korisničko ime i lozinku.
* D – Nakon što se korisnik uspješno prijavio, IdP generiše SAML token koji sadrži informacije o identitetu korisnika (kao što su korisničko ime, elektronska adresa itd.) IdP uzima taj token i preusmijerava korisnika nazad na davaoca usluga – SP (MyPhotos.com).
* E – MyPhotos.com provjerava SAML token, ukoliko je potrebno dešifruje ga i izdvaja informacije o identitetu korisnika – ko je taj korisnik i koje dozvole posjeduje. MyPhotos.com zatim korisnika prijavljuje u sistem, vjerovatno upotrebom kolačića ili kreiranjem nove sesije.

Na kraju procesa korisnik može koristiti MyPhotos.com kao prijavljeni korisnik. Pristupni podaci korisnika se nikada ne preslijeđuju kroz MyPhotos.com nego samo kroz IdP.

Postoji još detalja vezano za dijagram, ali ovo je opis onog što se dešava na visokom nivou.

### SAML token (Token) vs. SAML tvrdnja (Assertion)

Kada je SAML prvi put demonstriran, iznova i iznova se pojavljivao pojam *SAML token*. To u stvari i nije pojam definisan u okviru SAML specifikacije, ali je ostao u upotrebi iako njegovo značenje nije potpuno jasno.

Ispostavilo se da pojam *SAML token* predstavlja ustaljeni za upućivanje na SAML tvrdnju koja je često sabijen, kodirana, moguće i šifrovana i najčešće izgleda kao nešto zapetljano klupko. SAML tvrdnja je samo XML čvor sa određenim elementima.

### SAML ograničenja

SAML podržava koncept uvezivanja. To su u suštini sredstva kojim IdP preusmjerava korisnika nazad do SP. Npr. u koraku **D**, korisnik se preusmjerava nazad na MyPhotos.com, ali kako ?

Dva bitna tipa uvezivanja su HTTP preusmijeravanje (HTTP Redirect) i HTTP POST uvezivanja, navedena u SAML 2.0 specifikaciji. HTTP Redirect koristi HTTP preusmjeravanje kako bi poslao korisnika nazad na SP, u slučaju našeg primjera na MyPhotos.com

HTTP Redirekt je odličan za kratke SAML poruke, ali se ne preporučuje njegova upotreba ukoliko su poruke duge, kao što je SAML tvrdnja.

Preporučeni način uvezivanja tj. HTTP POST takođe ime svoje nedostatke. Npr. SAML specifikacija preporučuje da se u koraku D prikaže HTML forma sa akcijom koja upućuje nazad na SP.

Možete dodati dugmić na koji korisnik treba kliknuti kako bi poslao podatke sa forme ili koristiti JavaScript funkciju za automatizovano slanje. Zbog čega mora postojati forma koja se šalje? Razlog je što je u vremenu kada je izašla SAML 2.0 specifikacija bilo moguće to postići jedino upotrebom forme, tako da je bilo potrebno koristiti HTTP POST za slanje SAML tokena nazad do SP-a. U to vrijeme, to je bilo neophodno rješenje.

Međutim, to predstavlja problem u slučaju kada klijent nije web-bazirana aplikacije nego nativna aplikacija, kao što su mobilne aplikacije. Npr. recimo da smo instalirali MyPhotos aplikaciju za iPhone. Kada otvorimo aplikaciju, potrebna je autentifikacije posredstvom dobavljača identiteta. Nakon što se autentifikujemo, dobavljač identiteta treba poslati nazad SAML token do MyPhotos aplikacije.

Većina mobilnih aplikacija mogu biti pokrenute upotrebom prilagođenog URLa, kao što je npr. „my-photos://authenticate“, i najvjerovatnoje, dobavljač identiteta šalje formu koja sadrži SAML token na taj URL. MyPhotos aplikacija će se pokrenuti, ali nećemo biti ulogovani. Šta je razlog tome?

Mobilne aplikacije nemaju pristup HTTP POST tijelu. One imaju pristup samo URL-u koji se koristi za pokretanje aplikacije. To znači da ne možemo pročitati SAML token.

### Zaobilazno rješenje SAML HTTP POST uvezivanja

Ograničenje HTTP POST uvezivanja za mobilne aplikacije može biti riješeno na drugi način. Npr. moguće je koristiti ugrađene web prikaze, u okviru kojih se može napisati prilagođeni kod koji će nadgledati cijeli proces autentifikacije. Na završetku cjelokupnog potrebno je odstraniti nepotreban HTML kod i izvući SAML token.

Drugo zaobilazno rješenje je implementacija proxy servera koji može primiti HTTP POST, izvući SAML token, a zatim napraviti URL koji sadrži SAML token (npr. „myphotos://authenticate/?SAMLRequest=gfhvcmijtrra“). Proxy server bi zatim mogao upotrijebiti HTTP redirekciju kako bi doveo do toga da uređaj pokrene aplikaciju MyPhotos. Kako je sada SAML token dio URL-a, aplikacija MyPhotos ga može izdvojiti u upotrijebiti za prijavu.

Treće rješenje bi bilo zanemarivanje preporuke protiv upotrebe HTTP Redirect uvezivanja. Međutim ni malo se ne preporučuje jer je veoma lako napraviti pogrešan korak.

Još jedan pristup koji ne koristi zaobilazno rješenje je da se ne koristi SAML nego druga strategija kao što je OAuth 2.0.

## OAuth 2.0

Za razliku od SAML-a, OAuth 2.0 (nadalje OAuth2) je specifikacija koja je gotovo u potpunosti odbačena krajem 2012. godine. Ima olakšicu pošto je novija specifikacija i sve više se uzima u obzir kako se svijet tehnike mijenjao zadnjih osam godina.

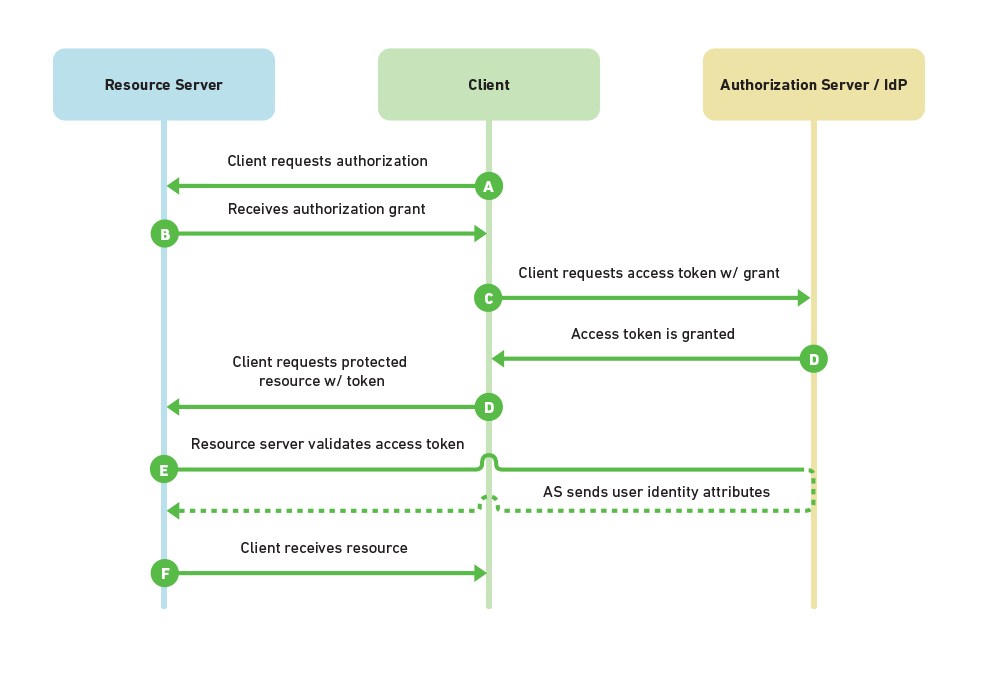
Mobilni uređaji i nativne aplikacije danas napreduju na način koji SAML nije mogao očekivati 2005. godine.

Ključni igrači OAuth2 su:

SAML i OAuth2 koriste slične pojmove za slične koncepte. Zbog poređenja, pored zvaničnog OAuth2 izraza u zagradama navodimo i ekvivalentan SAML izraz.

* Server resursa – Resource Server (Service Provider) – web server kome pokušavamo pristupiti.
* Klijent – Client – način na koji korisnik međudjeluje sa serverom resursa. To može biti web aplikacija u okviru pregledika, nativnam obilna aplikacija, desktop aplikacija serverska aplikacija itd.
* Autorizacijski server - Authorization Server (Identity Provider) - server koji posjeduje identitet i pristupne podatke korisnika, tj. potvrđuje identitet prava pristupa korisnika.

Na visokom nivou, OAuth2 scenario upotrebe se ne razlikuje mnogo od SAML-a:



Slika 8.2 - OAuth2 scenario upotrebe

Primjer slučaja upotrebe korišten i kod ranije opisanog SAML-a:

* A – korisnik otvara web preglednik i posjećuje MyPhotos.com na kome se nalaze sve njegove slike. MyPhotos.com ne može sam vršiti autentifikaciju korisnika tako da se on preusmjerava na autorizacijski server sa zahtjevom za autorizaciju. Korisniku se prikazuje forma za prijavu i traži se potvrda da želi odobriti serveru sa resursima (MyPhotos.com) da djeluje u njegovo ime. Korisnik se prijavljuje i zatim preusmjerava nazad na MyPhotos.com.
* B – klijent prima kod za odobrenje autorizacije kao dio preusmjeravanja
* C – klijent zatim koristi taj autorizacijski kod kako bi zahtijevao pristupni token od autorizacijskog servera
* D – ukoliko je kod za odobrenje autorizacije ispravan, autorizacijski server odobrava pristupni token. Pristupni token se zatim koristi od strane klijenta pri zahtijevanju resursa sa servera sa resursima (MyPhotos.com).
* E – MyPhotos.com prima zahtjev za resursom i pristupni token. Kako bi se uvjerio da je token ispravan, šalje ga direktno autorizacijskom serveru zbog provjere. Ukoliko je token ispravan, autorizacijski server šalje nazad informacije o korisniku.
* F – nakon provjere korisničkog zahtjeva MyPhotos.com šalje nazad korisniku zahtijevani resurs

Ovo je najčešći OAuth2 tok: tok autorizacijskog koda. OAuth2 nudi tri dodatna toka (kako ih oni zovu odobrenja autorizacije) koji su namijenjeni malo drugačijim scenarijima, kao što su JavaScript aplikacije u okviru jedne stranice, nativne mobilne aplikacije, nativne desktop aplikacije, standardne web aplikacije, serverske aplikacije.

Veliku prednost OAuth2 tokova je to što se komunikacija od autorizacijskog servera nazad do klijenta i servera sa resursima vrši putem HTTP preusmjeravanja (HTTP Redirect) zajedno sa informacijama o tokenu dostupnim u obliku parametara upita. OAuth2 takođe ne pretpostavlja da je klijent u stvari web preglednik, dok SAML Web Browser SSO Profile to radi.

Nativne mobilne aplikacije će odmah raditi, bez potrebe za zaobilaznim rješenjima.

### OAuth2 nedostaci

OAuth2 specifikacija u mnogim slučajevima ne propisuje kako radi komunikacija između resursnog servera i autorizacijskog servra, kao npr. u slučaju provjere tokena. Takođe ne govori ništa o tome koje informacije o korisniku bi trebale biti vraćene ni u kom obliku.

Postoji dosta mjesta gdje OAuth2 specifikacija navodi da su stvari „izvan okvira ove specifikacije (outside the scope of this specification)“. To je dovelo do kritika na OAuth2 specifikaciju jer su mnoge stvari prepuštene implementaciji, što bi u jednom trenutku moglo dovesti do nekompatibilne implementacije.

OAuth2 je još uvijek veoma mlad, a već je široko prihvaćen od strane Google-a, Facebook-a, Salesforce-a, Twitter-a i mnogih drugih. Istinska ljepota OAuth2 se ogleda u njegovoj jednostavnosti. U stvari, OpenID Connect Basic Profile, izgrađen na OAuth2, popunjava neke oblasti koje sama OAuth2 specifikacije ne definiše.

## Rezime – SAML vs. OAuth2

SAML posjeduje svojstvo koje nedostaje OAuth2: SAML token sadrži informacije o identitetu korisnika. Upotrebom OAuth2 te informacije nisu odmah direktno dostupne, te zbog toga resursni server mora napraviti dodatni zahtjev za provjeru tokena sa autorizacijskim serverom.

Sa druge strane, upotrebom OAuth2 moguće je poništiti pristupni token na autorizacijskom serveru, i onemogućiti njegovu dalju upotrebu na resursnom serveru.

Oba pristupa imaju korisne mogućnosti i oba će dobro poslužiti za implementaciju SSO-a.

OAuth2 nudi jednostavnije i više standarizovano rješenje kojim se izbjegavaju zaobilazna rješenja za podršku nativnih aplikacija.

# IMPLEMENTACIJA SSO SERVERA

Zadatak praktičnog dijela ovo rada je implementacija SSO servera sa osnovnim funkcionalnostima, koji omogućava autentifikaciju i autorizaciju korisnika.

Implementacija praktičnog dijela se sastoji od SSO servera tj. IdP-a te dva klijenta tj SP-a koji sluze za demonstraciju funkcionisanja samog servera. Razmjena autentifikacionih i autorizacionih poruka se vrši upotrebom SAML 2.0 protokola, i to na način koji definiše SAML 2.0 Web Browser SSO profil.

## Web Browser SSO profil

Ovaj profil podrazumijeva postojanje provajrdera identiteta (IdP), provajdera servisa (SP) i korisničkog agenta. Zavisno od načina povezivanja kojih SP posjeduje 4 a IdP 3, postoji ukupno 12 različitih scenarija. Za ovu implementaciju je korišten najčešći scenario u kome SP vrši slanje SAML zahtjeva koristeći redirekciju dok IdP vrši slanje odgovora putem HTTP POST metode.

Servis provajder - SP

(SSO klijent)

Korisnički agent

(web preglednik)

Provajder identiteta - IdP

(SSO servis)

**8**

**7**

**6**

**5**

**4**

**3**

**Preusmjerava na željeni resurs**

**Preusmjerava na željeni resurs**

**Zahtjeva željeni resurs**

**Zahtjeva servis za konzumiranje odgovora**

**Odgovara XHTML formom**

**(Identifikuje korisnika)**

**Zahtjeva SSO servis**

**1**

**Zahtjeva željeni resurs**

**(Pronalaženje IdP-a)**

**Preusmjerava na SSO servis**

**2**

U narednim tačkama su objasnjeni gore navedeni koraci. Korištene se adrese i primjeri poruka relaizovane implementacije.

1. **Zahtjevanje željenog resursa**

Korisnik putem svog web preglednika zahtjeva željeni resurs na strani servis provajdera (koji predstavlja web aplikaciju)

https://localhost:8081/sp1/protectedResource

Servis provajder vrši provjeru prava pristupa željenom resursu. Ako već postoji važeći sigurnosni kontekst, preskaču se koraci od 2 do 7.

1. **Preusmjeravanje na IdP SSO servis**

Servis provajder generiše odgovarajući SAML zahtjev (i RelayState parametar), a zatim preusmjerava preglednik korisnika na SSO servis koristeci standardnu HTTP redirekciju.

302 Redirect

Location:https://localhost:8080/sso/Redirect?SAMLRequest=<request>&RelayState=<relystate>

SAMLRequest može biti potpisan, ali za onovni primjer nije. Parametar RelayState predstavlja neprozirnu referencu ka stanju informacija koje se čuvaju na strani servis provajdera. U ovoj implementaciji sluzi za čuvanje reference ka informaciji na strani servisnog provajdera koja predstavlja traženi resurs, kako bi se nakon autentifikacije na SSO strani korisnik automatski preusmjerio na taj resurs.

SAMLRequest parametar je kompresovan, base64 enkodiran i URL enkodirana vrijednost <samlp:AuthnRequest> elementa:



1. **Zahtjevanje SSO servisa na IdP strani**

U skladu sa HTTP standardom, web preglednik šalje GET zahtjev SSO servisu na IdP strani:

GET /Redirect?SAMLRequest=<request>&RelayState=

<relystate> HTTP/1.1

Host: localhost:8080/sso

Vrijednosti parametara SAMLRequest i RelayState su iste kao one proslijedjene od strane servis provajdera. SSO servis na IdP strani procesira <samlp:AuthnRequest> element tako što ga prvo URL-dekodira, base64-dekodira te dekompresuje (tim redosledom) a zatim vrši sigurnosnu provjeru. Ako korisnik nema važeći sigurnosni kontekst, IdP identifikuje korisnika nekim od mehanizama autentifikacije, tj u ovom slučaju login formom.

1. **Odgovor XHTML formom**

SSO servis nakon validiranja zahtjeva odgovara stranicom koja sadrži XHTML formu:

<form method=”post” action=”http://localhost:8081/sp1/saml”>

<input type=”hidden” name=”SAMLResponse” value=<samlres> />

<input type=”hidden” name=”RelayState” value=<relstate> />

...

<input type=”submit” value=”Submit”>

</form>

Vrijednost RelayState parametra je očuvana jos iz 3. koraka. Vrijednost SAMLResponse parametra je base64 enkodiran <samlp:Response> element:



1. **Zahtjevanje servisa za konzumiranje odgovara na SP strani**

Preglednik korisnika šalje POST zahtjev servisu za konzumiranje odgovora na strani servis provajdera.

POST /saml HTTP/1.1

Host: localhost:8081/sp1

Content-Type: application/x-www-form-urlencoded

SAMLResponse=response&RelayState=token

gdje su vrijednosti SAMLResponse i RelayState parametara uzete sa XHTML forme.

1. **Preusmjeravanje na željeni resurs**

Servis za konzumiranje odgovora obradjuje odgovor, stvara sigurnosni kontekst na strani servis provajdera i preusmjerava korisnika na željeni resurs koristeći referenu smještenju u RelayState parametru.

1. **Novi zahtjev za željeni resurs na strani SP-a**

Korisnik upotrebom preglednika ponovo zahtjeva novi resurs na strani servis provajdera:

https:// localhost:8081/sp1/protectedResource2

1. **Odgovor vraćanjem željenog resursa**

S obzirom na to da već postoji sigurnosni kontekst, servis provajder vraća zahtjevani resurs.

## Integracija SSO klijenata sa SSO serverom

U ovom dijelu objasnićemo od čega se sastoje klijent i server aplikacije, kako je izvršena integracije i konfigurisanje klijent aplikacija za konzumiranje SSO servera, te na koji način se stvara sigurnosni kontekst na strani klijenta.

Kao što je ranije navedeno, praktični dio ovo rada čine dvije ServiceProvider (SP) aplikacije koje predstavljaju klijente i IdentificationProvider koji predstavlja SSO server na koji se klijentske aplikacije povezuju.

SP aplikacije su implementirane su kao veoma jednostavne Spring Boot aplikacije koje služe za demonstrativnu srvhu, kako bi se pokazalo i testiralo autentifikovanje i autorizovanje putem SSO servera. Sadrže smo dvije stranice, tj početnu stranicu koja je nezaštićena tj pristup je omogućen svim korisnicima, te testnu stranicu koja je zaštićena i zahtjeva da korisnik bude autorizovan sa određenom rolom odnosno ulogom.

IdP aplikacija je takodje Spring Boot aplikacija, povezana sa bazom podataka čija se struktura vidi na narednoj slici. Sastoji se samo od login stranice koja se prikazuje ukoliko korisnik (preusmjeren na IdP od strane SP-a) još uvijek ne posjeduje važeći sigurnosni kontekst na IdP strani, tj nije autentifikovan. Za kreiranje SAML poruka koristi se OpenSAML biblioteka. IdP aplikacija sadrži Maven plugin koji kreira JAR paket koji se koristi u okviru klijentskih aplikacija kako bi se pripremile sve neophodne stvari za komunikaciju sa IdP-om. Ovaj paket sadrži metodu sa kreiranje AuthnRequest poruka i pripremu za slanje putem redirekcije, metodu za generisanje odgovarajuće HTTP redirekcije koja sadrži tačnu putanju do IdP-a te metodu za konvertovanje SAML odgovora u odgovarajući Response objekat iz OpenSAML biblioteke.



Tabele users i user\_roles su tabele koje Spring Security koristi kako bi authentifikovao i autorizovao korisnika na strani IdP-a, odnosno nad ovim tabelama se vrše upiti prilikom autentifikacije korisnika na SSO serveru nakon redirekcije od SP-a. Tabele target\_hosts i target\_authorities sadrže autorizacijske podatke koje autentifikovani korisnik posjeduje na određenim SP aplikacijama odnosno klijentima.

### Pozadinski proces prilikom pristupa zaštićenoj stranici na strani SP-a

1. Korisnik putem preglednika pristupa početnoj stranici prve SP1 aplikacije – localhost:8081/sp1, pri čemu mu se otvara stranica sa objašnjenjem i linkom za zaštićenu stranicu
2. Kada korisnik klikne na link za zaštićenu stranicu, aplikacija detektuje da ne postoji sigurnosni kontekst neophodan da se se korisniku prikaže stranica. Usled toga na SP strani se kreira SAML zahtjev koji predstavlja AuthnRequest element. Uz kreiranje zahtjeva, generiše se i RelayState vrijednost koja se čuva u mapi zajedno sa adresom prethodno traženog resursa tj stranice, kako bi se nakon povratka sa SSO servera korisnik mogao automatski redirektovati na nju. Kada je sve spremno, prethodno generisane vrijednosti se koriste kako bi se poslala HTTP redirekcija na SSO server.

SAML zahtjev se prvo kompresuje, base64 enkodira i URL enkodira i ta vrijednost se salje kao SAMLRequest parametar redirekcije. Uz to se dodaje i RelayState parametar koji predstavlja referencu na informacije u mapi na strani SP-a. Konačno, vrši se redirekcija korisnika na SSO server, i to na putanju koja je konfigurabilna, a predstavlja komponentu SSO servera koja obrađuje SAML zahtjeve.

1. Prilikom redirekcije, korisnik se šalje na IdP putanju koja vrši obradu AuthnRequest zahtjeva – localhost:8080/sso/Redirect. Medjutim, ova putanja je takodje zaštićena, a pošto korisnik još nema važeći sigurnosni kontekst na IdP strani, prikazuje mu se stranica za autentifikaciju na SSO server. Na toj stranici potrebno je unijeti pristupne podatke, tj korisničko ime i lozinku čije se postojanje zatim provjerava u bazi.

Nakon što se uspješno autentifikuje, korisnik dobija važeći sigurnosni kontekst na strani IdP-a, tako da dobija pristup localhost:8080/sso/Redirect putanji. Kako se na ovoj putanju nalazi komponenta koja vrši obradu zahtjeva, iz AuthnResponse-a se izvlači podatak o servisnom provajderu tj clijentu koji je uputio zahtjev za autorizaciju korisnika. Prije svega, AuthnResponse se mora prvo URL dekodovati, base64 dekodovati i dekompresovati. S obizirom na to da znamo ko je prethodno autentifikovani korisnik i koji servisni provajder je izdao zahtjev, IdP u bazi pronalazi koja prava pristupa korisnik ima na tom provajderu, tj prikuplja uloge odnosno role tog korisnika. Ova informacija se dodaje kao vrijednost Attribute elementa pod nazivom „role“ koji se nalazi pod AttributStatement elementom SAML odgovora. Kasnije će SP1 na osnovu ove vrijednosti znati koja su prava pristupa korisnika.

Nakon što je SAML Response kreiran i popunjen, nad njegovim String oblikom se vrši base64 enkodovanje. Ta vrijednost se dodaje kao atribut XHTML forme zajedno uz nepormijenjenu RelayState vrijednost, podaci se šalju nazad do SP-a HTTP POST metodom. Adresa na koju se šalju podaci je poznata tako što IdP izvači vrijednos Issuer elementa iz AuthnRequest-a.

1. Kada HTTP POST zahtjev stigne na ciljanu putanju na SP-u, u ovom slučaju na localhost:8081/sp1/saml koja predstavlja tzv „Assertion Consumer Service“, tj servis za konzumiranje SAML odgovora vrši se njegova obrada. Prvi korak obrade odgovora je njegova validacija koja se vrši provjeravanjem određenih informacija kao što su vrijeme kreiranja i krajnje vrijeme do kog je odgovor važeći, itd.

Ukoliko je odgovor validan, SP1 izdvaja role za datog korisnika i na osnovu tih rola za njega kreira odgovarajući sigurnosni kontekst, u našem slučaju Spring Securty kontekst sa datim rolama. Ovim je korisnik autentifikovan i autorizovan u okviru SP1 aplikacije. Nakon toga, na osnovu RelayState state vrijednosti koja je takodje primljena kao dio HTTP odgovora, SP pronalazi inicijalno željenu stranicu kojoj je korisnik želio pristupiti i vrši redirekciju korisnika na tu stranicu. Ukoliko se neka od rola koje korisnik posjeduje poklapa sa rolama potrebnim za pristup stranici, korisnik će je uspješno vidjeti, u suprotnom, dobiće stranicu sa porukom Access Denied.

1. Ako korisnik pokuša da pristupi nekoj drugoj zaštićenoj stranici u okviru SP1 aplikacije, izvršiće se provjera postojanja važećeg sigurnosnog konteksta u okviru te aplikacije. Ukoliko kontekst već postoji pošto je kreiran u prethodnom koraku, SP1 neće slati novi SAML zahtjev SSO serveru tj IdP-u nego će odlučiti o pravima pristupa željenoj stranici na osnovu postojećeg sigurnosnog konteksta.
2. Ukoliko taj isti korisnik sada pokuša da pristupi zaštićenoj stranici u okviru druge klijentske aplikacije SP2 na kojoj još nema sigurnosni kontekst, ponoviće se svi prethodno navedeni koraci, s tim da na IdP strani neće morati ponovo da unosi pristupne podatke jer već postoji sigurnosni kontekst za tog korisnika na strani IdP-a. Na taj način će korisnik biti automatski redirektovan na SP2, gdje će mu biti kreiran sigurnosni kontekst sa odgovarajućim rolama, odnosno biće autentifikovan i autorizovan i u okviru druge klijentske aplikacije.

# ZAKLJUČAK

# LITERATURA

1. <https://auth0.com/blog/what-is-and-how-does-single-sign-on-work/>
2. <http://www.tomsitpro.com/articles/single-sign-on-solutions,2-853.html>
3. <http://docs.media.bitpipe.com/io_12x/io_122457/item_1111347/03-0615_HB_Making%20Sign-on%20Simple%20and%20Secure.pdf>
4. <https://www.icann.org/news/blog/what-is-authorization-and-access-control>
5. <https://www.owasp.org/index.php/Category:Access_Control#Definition>
6. <https://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html>
7. <https://community.emc.com/docs/DOC-7314>
8. <https://www.mutuallyhuman.com/blog/2013/05/09/choosing-an-sso-strategy-saml-vs-oauth2/>
9. <http://tech-nugget.blogspot.rs/2013/09/saml-explained.html>
10. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
11. <http://wiki.servicenow.com/index.php?title=SAML_2.0_Web_Browser_SSO_Profile#gsc.tab=0>
12. <http://saml.xml.org/wiki/sp-initiated-single-sign-on-postartifact-bindings>
13. <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-single-sign-on-protocol-reference>
14. [https://en.wikipedia.org/wiki/SAML\_2.0#SP\_POST\_Request.3B\_IdP\_POST\_Response](https://en.wikipedia.org/wiki/SAML_2.0%23SP_POST_Request.3B_IdP_POST_Response)

1. *Organization for the Advancement of Structured Information Standards* (OASIS) je međunarodna neprofitna organizacija koja radi na razvoju, širenju i usvajanju standarda u oblastima sigurnosti, interneta stvari, energije, upravljanja hitnim slučajevima itd. [↑](#footnote-ref-1)