**UNIVERZITET U BANJOJ LUCI**

**ELEKTROTEHNIČKI FAKULTET**

**Rajo Gajić**

**REALIZACIJA SSO SERVERA**

**Diplomski rad**

**Banja Luka, 2016**

**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

# UVOD

U današnje vrijeme gotovo svaki web sajt zahtjeva neki oblik provjere identiteta za pristup sadržajima i funkcionalnostima. Sa povećanjem broja sajtova i servisa, centralizovani sistem za prijavu korisnika postaje nužnost. „Single-sign-on“ (SSO) je sada potreban vise nego ikada.

Koncept centralizovanog ili povezanog elektronskog identiteta poznat je kao ujedinjeni identitet. Sistemi ujedinjenog identiteta upravljaju sa sledećim problemima:

* Autentifikacija (provjera identiteta)
* Autorizacija (prava pristupa)
* Razmjena korisničkih atributa
* Upravljanje korisnicima

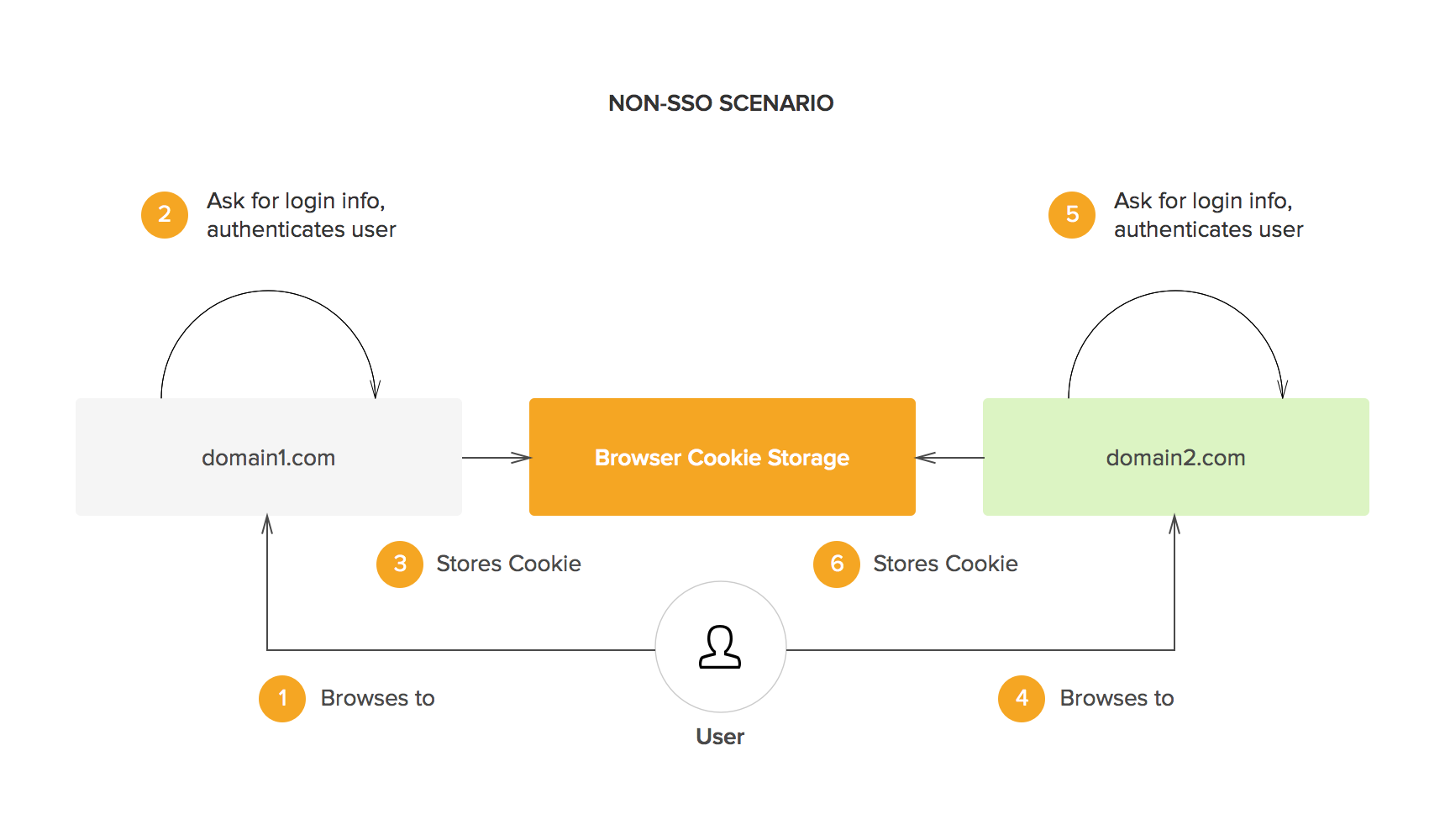
**Autentifikacijski** aspekt se zasniva na provjeri pristupnih podataka i na identifikaciji korisnika. **Autorizacija** je vezana za prava pristupa (npr. da li korisnik ima dozvolu da pristupi određenom resursu). **Razmjena korisničkih atributa** predstavlja dijeljenje informacija o korisniku između različitih sistema za upravljanje korisnicima. Na primjer, atribut „pravo ime“ može biti prisutan u nekoliko sistema. Sistem centralizovanog identiteta spriječava dupliranje podataka povezivanjem ekvivalentnih atributa u različitim sistemima. Na kraju, **upravljanje korisnicima** je vezano za administraciju (dodavanje, brisanje, ažuriranje) korisničkih naloga. Ovaj sistem omogućuje administratorima (ili korisnicima) da održavaju jedan korisnički nalog u okviru više domena ili podsistema.

SSO je isključivo povezan sa **autentifikacijskim** dijelom sistema centralizovanog identiteta. Osnovni zadatak SSO servera je identifikacija korisnika i dijeljenje tih podataka sa svim podsistemima koji zahtijevaju podatke.

# Single-sing-on (SSO)

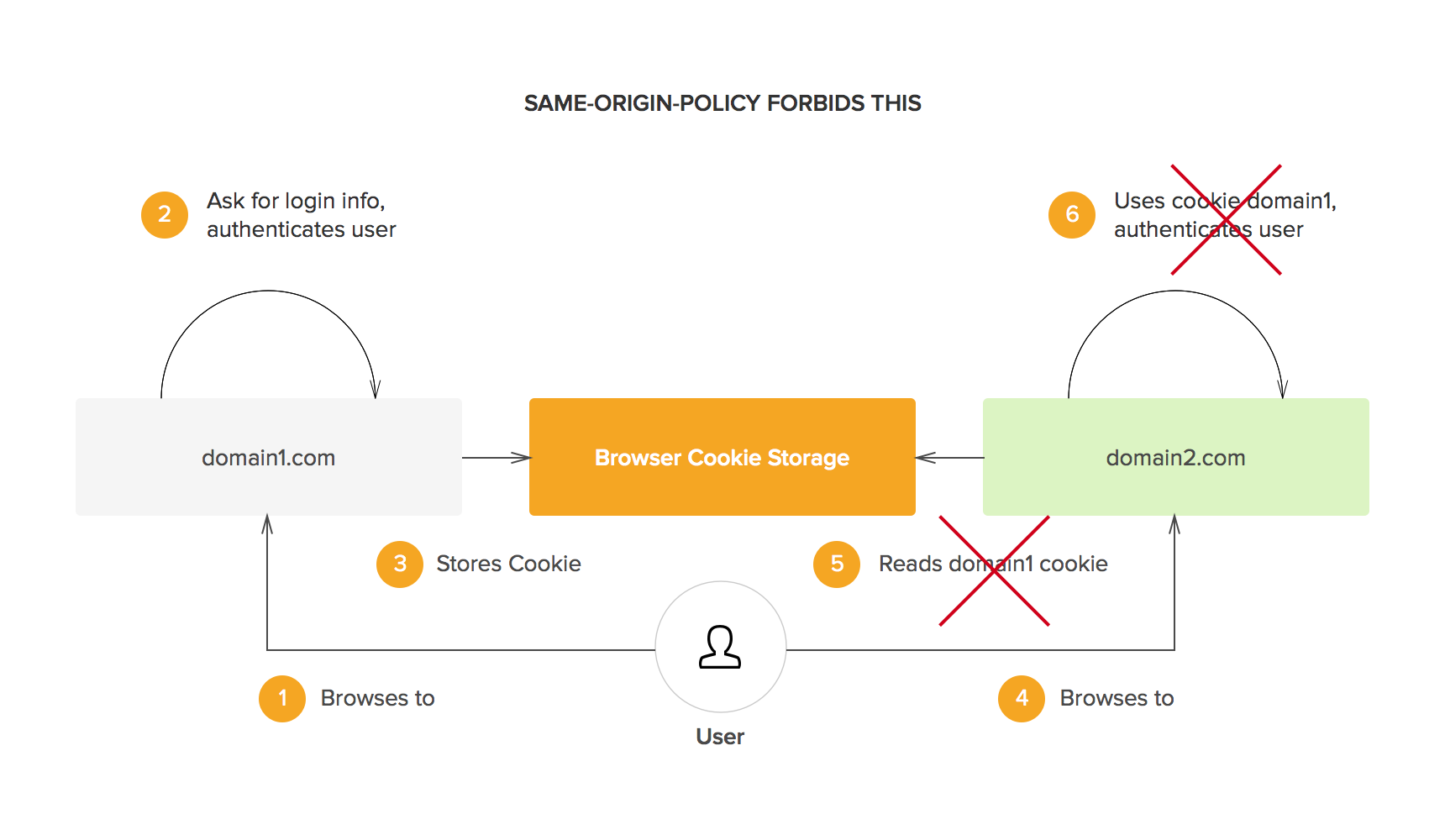
Prije ili kasnije razvojni tim naiđe na jedan problem: razvili ste aplikaciju na domenu X a sada želite da vaša nova aplikacija na domenu Y koristi iste pristupne podatke kao i domen X. U suštini, želite i više: da korisnici koji su već prijavljeni pod domenom X budu automatski prijavljeni i pod domenom Y. To je osnovni zadatak SSO servera.

Npr. Google je realizovao SSO za svoje proizvode: Gmail, YouTube, Analytics itd. Kada na svom računaru pristupite Gmail aplikaciji, ulogujete se prvi put, a zatim posjetite YouTube, nećete morati ponovo unositi pristupne podatke nego ćete biti automatski prijavljeni.



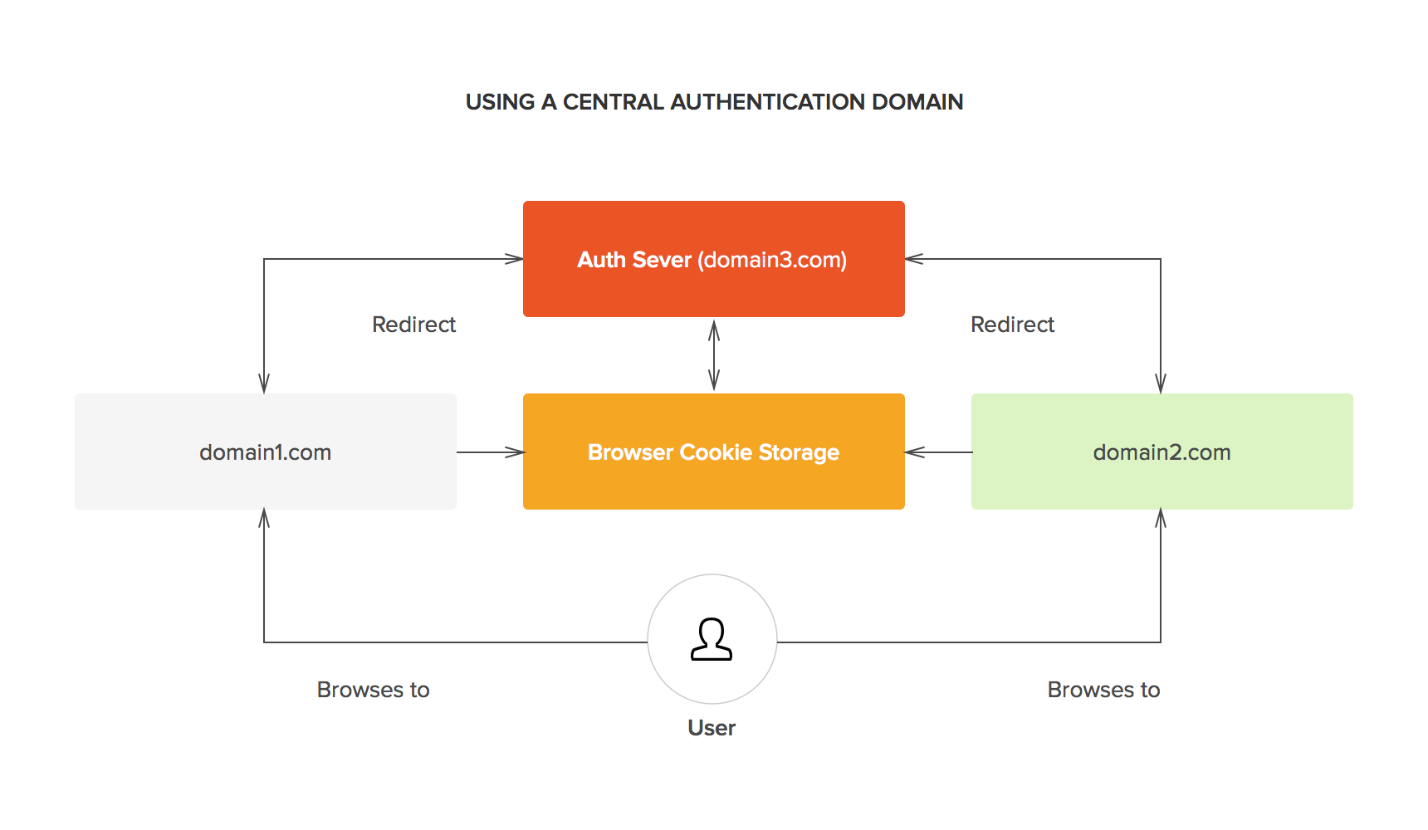
Slika 1 – Rješenje bez SSO servera

Očigledno rješenje ovog problema je dijeljenje informacija o sesijama između različitih domena. 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.



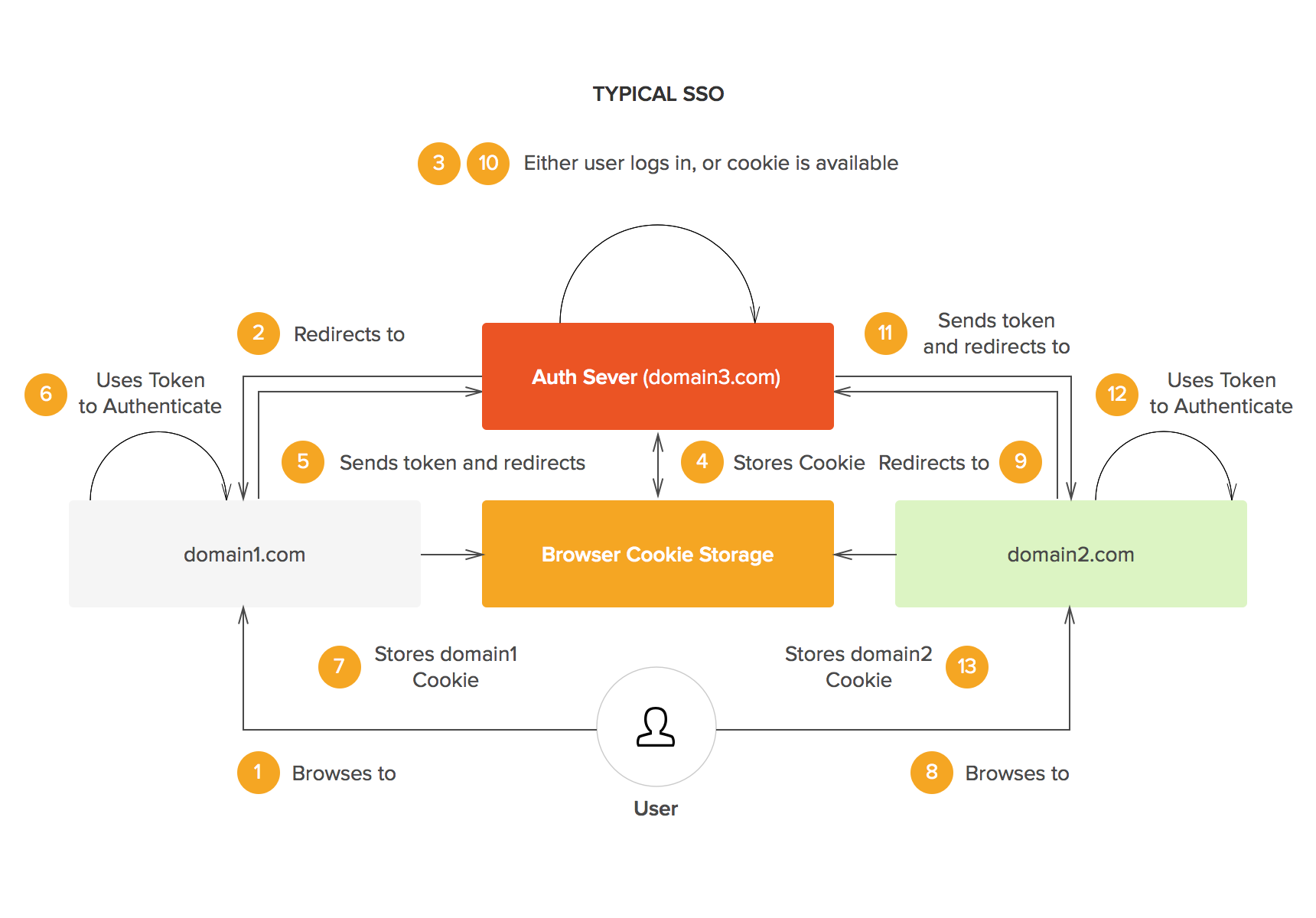
Slika 2 - Pravilo istog porijekla

Različiti SSO protokoli dijele sesijske podatke na različite načine, ali osnovni princip je isti – postoji centralni domen preko kog se vrši autentifikacija, nakon čega se sesija dijeli sa ostalim domenima na neki način. Npr. centralni domen generiše potpisani JSON Web Token (koji može biti šifrovan upotrebom JWE). Taj token se dalje može proslijediti klijentu i može se koristiti od strane autentifikacijskog 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 autentifikaciju. S obzirom na to da je token potpisan, ne može biti izmijenjen od strane klijenta ni na koji način.



Slika 3 - Upotreba centralnog autentifikacionog domena

Svaki put kada korisnik posjeti domen koji zahtjeva autentifikaciju, redirektovan je na autentifikacijski domen. S obzirom na to da je korisnik već ulogovan pod tim domenom, može odmah biti redirektovan na izvorni domen uz neophodni autentifikacijski token.



Slika 4 - Uobičajeni SSO

Single sign-on (SSO) je oblik tehnologije koji olakšava proces autentifikacije 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 dodjeljuju prava pristupa određenim aplikacijama, i biće 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 autentifikacija izvršava u okviru posebnog servera za tu namjenu. Svi autentifikacioni podaci moraju prvo proći kroz poseban server za SSO, koji zatim dalje proslijeđuje određene autentifikacione informacije koje posjeduje za datog korisnika. Ovakav način centralizovanog sistema za autentifikaciju će vjerovatno prije odoljeti napadima i zlonamjernom pristupu nego obični sistem autentifikacioni 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.

# Autentifikacija

Autentifikacija je proces utvrđivanja da li je neko stvarno onaj za koga se predstavlja. Pri tom procesu pristupni podaci se porede sa onim u bazi ili nekom drugom izvoru liste podataka registrovanih tj. ovlaštenih korisnika. Ako se pristupni podaci poklapaju, proces autentifikacije je uspješno završen i korisnik dobija ovlašćenje za pristup sistemu.

Autentifikacija može biti sprovedena upotrebom pristupnih podataka, SSO sistema, biometrijski, digitalnim sertifikatima i javnim ključevima.

Autentifikacija korisnika je ključna za osiguravanje odgovarajućih ovlašćenja i pristupa sistemima i uslugama, naročito od kada je sve učestalija krađa podataka i sve su veće prijetnje sigurnosti informacija. Iako autentifikacija ne može u potpunosti spriječiti krađu informacija i identiteta, možemo se pobrinuti da naši resursi budu zaštićeni upotrebom nekoliko autentifikacijskih metoda.

## Autentifikacija upotrebom lozinke

U privatnim i javnim računarskim mrežama (uključujući internet), autentifikacija 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 na početku upotrebe sistema registruje (ili ga je već neko registrovao, npr. sistem administrator), upotrebom dodijeljene ili lozinke po svom izboru. Međutim, autentifikacija na osnovu lozinke se ne smatra dovoljno sigurnom i pouzdanom za bilo koji sistem koji sadrži osjetljive podatke.

Korisnička ima su često kombinacija imena i prezimena osobe, zbog čega ih je lako pogoditi. Ako se ne postave pravila za kreiranje, ljudi često prave prave slabe lozinke – čak i jake lozinke mobu biti ukradene, slučajno otkrivene ili zaboravljane. Iz tog razloga, internet poslovanje i mnoge druge transakcije zahtijevaju strože procese i metode autentifikacije.

Nedostaci autentifikacije na osnovu lozinke može 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 autentifikaciju na osnovu lozinke i generalno autentifikaciju na osnovu nečega što znamo su mnogo ranjiviji nego oni koji koriste nekoliko nezavisnih metoda autentifikacije.

Autentifikacioni faktor (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 nasleđivanja).

## Autentifikacioni faktori

* Faktori znanja – kategorija identifikatora koja sa sastoji od informacija koje korisnik posjeduje, 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 generise token
* Faktori nasleđivanja – kategorija identifikatora koja se sastoji od elemenata koji su svojstveni pojedincu, u obliku biometrijskih podataka kao što je npr. otisak prsta

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

# Upravljanje identitetima

Upravljanje identitetima je široka administrativna oblast koja se bavi identifikovanjem individua u sistemu i kontrolisanjem njihovog pristupa resursima u okviru tog sistema na osnovu povezivanja korisničkih prava sa utvrđenim identitetom.

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 upravljaju 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.

Upravljanje identitetima bavi se sledećim ključnim oblastima: upravljanje identitetima, kontrolom pristupa i directory services.

Što se tiče upravljanja identitetima (nalozima i korisničkim pristupom), postoje mnogi izazovi za pravilno upravljanje identitetima. Neki od njih uključuju kreiranje naloga, kao i njihovo održavanje i uklanjanje. Drugi izazov je, koji je najbolji način da se obezbijedi autentifikacija za korisnike. To može obuhvatati pravila vezana za lozinke i/ili biometriju. Kako potvrđujemo korisničke podatke na taj način da zaštitimo kompaniju, pri čemu istovremeno umanjujemo napor potreban kako bi se korisnik autentifikovao u okviru više sistema.

Uz povećanje broja sistema koji se koriste, povećava se i napor potreban za administraciju naloga. To je mjesto gdje SSO i upravljanje identitetima nastupaju zajedno. Odogvarajuća implementacija takvog sistema će značajno umanjiti cijelokupan administrativni posao neophodan pri upravljanju korisničkim informacijama u centralizovanom skladištu. Neki od problema koje ovakav sistem rješava:

* 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 više grupa
* Suvišne ili netačne informacije koje djelimično identifikuju direktorije i identitete

Možda najveći problem predstavlja to što neke kompanije adresiraju taj problem, ali ne poduzimaju ništa kako bi ga riješile, ne gledajući dugoročno i ne pokušavajući da se suoče sa stvarnim uzrokom problema.

Aplikacije mogu koristiti SSO kako bi obezbijedile korisnicima jednostavan i brz pristup sadržaju koji se čuva i uređuje na različitim vrstama sistema. To se postiže na taj način što se omogućava višestruka prijava sa istom lozinkom. SSO je metodologija koja obezbjeđuje jednu akciju za autentifikaciju i autorizaciju. Omogućuje korisnicima pristup svim računarima i sistemima na kojima imaju pravo pristupa, bez potrebe da unose lozinku više puta. Nudeći tu mogućnost, SSO značajno umanjuje ljudsku grešku, najčešći uzrok pada sistema. Moglo bi se reći da je najznačajnija stvar posjedovanja centralizovanog sistema, postojanje centralnog skladišta gdje se čuvaju sva korisnička imena i lozinke. SSO rješava problem postojanja pojedinačnih baza korisnika, lozinki i dozvola u okviru svake od aplikacija. Povezivanje grupe aplikacija upotrebom integrisanog sistema, omogućava i internim i eksternim korisnicima da koriste isto korisničko ime i lozinku za više različitih sajtova aplikacija.

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. Sve ovo je zavisno od odgovarajuće funkcionalnosti konzole za upravljanje, uključujući definisanje pravila, izvještavanje, upozorenja, alarme i ostale uobičajene zahtjeve upravljanja i operacija. Npr. alarm se može aktivirati kada određeni korisnik pokuša pristupiti resursu za koji nema dozvolu. Izvještavanje proizvodi revizijski dnevnik u koji se bilježe sve specifične aktivnosti koje su izvršene.

# Autorizacija i kontrola pristupa

Autorizacija je proces dodjeljivanja dozvole nekome da uradi ili posjeduje nešto. U višekorisničkim računarskim sistemima, sistem administrator definiše koji korisnici imaju pristup sistemu i koje privilegije posjeduju (kao što su pristup određenim direktorijima, trajanje i vrijeme pristupa, količina skladišnog prostora itd.). Pretpostavimo da se neko prijavi u računarski operativni sistem ili aplikaciju, sistem ili aplikacija identifikuju kojim resursima korisnik može pristupiti tokom sesije. Prema tome, autorizaciju možemo posmatrati i kao početna podešavanja dozvola od strane sistem administratora i kao provjeru dozvola koje se dodjeljuju korisniku kada dobije pristup.

Nakon autentifikacije, korisnik mora dobiti dozvolu za izvršavanje određenih zadataka. Npr. nakon prijave na sistem, korisnik može pokušati da izvrši neke komande. Autorizacijski proces određuje da li korisnik ima pravo da izvrši takvu komandu. 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 autentifikacije. Nakon što se korisnik autentifikuje, mogu mu se odobriti različiti tipovi pristupa ili aktivnosti.

??

Autentifikacija 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 da samo taj korisnik ima pravo pristupa svom ličnom nalogu nakon što se potvrdi njegov identitet.

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 ovi 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 autentifikuju 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 kada napravite dijeljeni direktorijum na svom laptopu.

Kontrola pristupa

Dok autorizacijska pravila definišu čemu određeni korisnik ili grupa korisnika može pristupiti, kontrola pristupa, takođe poznata pod nazivima dozvole ili privilegije, predstavlja metode koje sprovode autorizacijska pravila. Neki od primjera:

* Kroz podešavanja Facebook-a – Ko može vidjeti moje stvari ? Ko me može kontaktirati ? Ko me može pronaći ? – Nekim korisnicima ili javnosti dozvoljavam ili onemogućujemo pristup onome što postavaljamo na svoj Facebook nalog
* Podešavanja Google Docs-a omogućavaju nam postavljanje dozvola za izmjenu ili dijeljenje dokumenata koje zajednički koristimo
* Flickr podešavanja nam dozvoljavaju da kreiramo ili podijelimo album ili sliku sa porodicom, prijateljima ili sa javnošću

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

# SAML (Security Assertion Markup Language)

Jedno od najvažnijih bezbijednosnih pitanja je autentifikacija korisnika – konkretno, dozvoliti korisniku da se prijavi ili koristi nekoliko različitih ali uvezanih web sajtova ili servisa, bez potrebe da se pri tome svaki put ponovo autentifikuje. To je posao za SAML (Security Assertion Markup Language), autentifikacijski i autorizacijski standard zasnovan na XML-u (Extensible Markup Language) koji obezbjeđuje SSO, tako da se korisnici mogu samo jednom autentifikovati kako bi dobili pristup na nekoliko različitih web sajtova. SAML dozvoljava svakom od sajtova da posjeduje svoj mehanizam za prijavu i autentifikaciju, ali uvodi mogućnost prihvatanja autentifikovanih korisnika sa drugih sajtova.

## Zašto SAML

Prije nego što vidimo kako SAML funkcioniše, pogledajmo zbog čega je potreban. Recimo da neko posjeti sajt avio kompanije, prijavi se i rezerviše karte. Sajt nudi specijalne popuste za odsjedanje u hotelu ili iznajmljivanje automobila posredstvom partnerskih sajtova, i korisnik se odluči da izvrši rezervaciju. Kako bi izvršio rezervaciju na svakom od partnerskih sajtova, bez upotrebe SAML-a, korisnik se mora pojedinačno prijaviti na svaki od sajtova, upotrebom različitih korisničkih imena i lozinki. Takođe postoji vjerovatnoća da mora unositi specijalne promo kodove kako bi potvrdio da ima pravo na određeni popust. Ali uz upotrebu SAML-a, korisnik bi se trebao prijaviti samo jednom na prvom sajtu tj. na sajtu avio kompanije, nakon čega bi automatski bio autentifikovan posredstvom SAML-a i na uvezanim partnerskim sajtovima.

Još problematičnije su složene B2B (business-to-business) transakcije koje se obavljaju preko web servisa. Web servisi se najčešće koriste u automatizovanim transakcijama koje obuhvataju višestruke poslovne partnere, uključujući proizvođače, distributere, prevoznike, dobavljače i trgovce. Bez načina da se autentifikuje svaki partner i šta svako od njih može ili ne može vršiti u okviru transakcije, ne bi ih bilo moguće automatizovati. Uz SAML koji upravlja autentifikacijom, složene transakcije mogu biti automatizovane bez razmišljanja o problemima autentifikacije.

## Kako SAML funkcioniše

Na koji način SAML rješava sve ? U suštini, SAML nije nišsta više nego niz XML baziranih poruka koje govore da li je korisnik autentifikovan, kakva prava, uloge i pristupe posjeduje te na koji način može koristiti podatke i resurse na osnovu tih prava i uloga. Kompatibilan je sa HTTP, SMTP, FTP i SOAP protokolima, uz niz ostalih protokola i tehnologija.

Tri glavne komponente SAML specifikacije su:

* **Tvrdnje** – SAML posjeduje tri vrste tvrdnji. Tvrdnje autentifikacije su one u kojima je korisnik dokazao svoj identitet. Atributske tvrdnje sadrže određene informacije o korisniku, kao što je npr. ograničenje troškova. Autorizacijske tvrdnje opisuju šta korisnik može raditi, npr. može li kupovati proizvode
* **Protokol** – definiše način na koji SAML zahtijeva i prima tvrdnje, npr. upotrebom SOAP-a posredstvom HTTP-a, iako postoje i duge metode
* **Vezivanje** – detaljno opisuje način na koji se razmijene SAML poruka mapiraju u SOAP razmijene. SAML podržava više protokola uključujući HTTP (Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol) i takođe podržava SOAP, BizTalk i ebXML (Electronic Business XML)

**Tvrdnje** se razmjenjuju između sajtova i servisa upotrebom **protokola** i **vezivanja** – one autentifikuju korisnika između različitih sajtova.

## SAML u upotrebi

Kako SAML funkcioniše u stvarnosti. Pogledajmo konkretan primjer njegove upotrebe. Recimo da se neko prijavi i autentifikovan je na web sajt koji koristi, nakon čega želi posjetiti sajt partnera. Upotrebom SAML-a, može biti autentifikovan i u okviru drugog sajta bez potrebe da se prijavi. Sledeći primjer pokazuje svaki korak procesa:

* U prvom koraku korisnik se autentifikovao u okviru Sajta 1 i želi posjetiti Sajt 2. Klikće na link kako bi otišao na njega.
* U drugom koraku, umjesto da bude direktno poslan na Sajt 2, šalje se na SAML servis Sajta 1.
* U trećem koraku SAML servis dodaje ID partnera i dodatne parametre na URL Sajta 2 u okviru preglednika korisnika. Npr. ako korisnik posjeti sajt <http://www.ebay.com>, nakon što SAML servis prikači dodatne informacije, URL bi mogao biti <https://www.ebay.com?SAMLart>= . Možemo primijetiti da se protokol prebacio na zaštićeni HTTPS umjesto standardnog HTTP. Korisnik se sada preusmjerava na SAML servis Sajta 2, koji ispituje URL sa dodatnim parametrima. Na osnovu parametara URL-a, SAML servis Sajta 2 komunicira sa Sajtom 1 koji proslijeđuje autentifikovani identitet korisnika, zajedno sa svim pravima koje korisnik posjeduje.
* U zadnjem koraku, korisnik se šalje na Sajt 2, gdje je u potpunosti autentifikovan. On sada može izvršavati transakcije u okviru toga sajta, baš kao da se direktno prijavio na njega.

## SAML 2.0

OASIS je 19. Augusta 2004 godine izbacio grubu specifikaciju SAML-a 2.0. Poboljšanja koje je donijela nova verzija:

* Podrška za sesije – kreiranje, održavanje i uklanjanje kako bi se održalo jedinstveno sigurnosno okruženje
* Razmjena metapodataka (podataka o podacima) o tvrdnjama, protokolima za slanje poruka i formatima, kako bi se obezbijedilo bolje međudjelovanje

# XACML (Extensible Access Control Markup Language)

XACML (Extensible Access Control Markup Language) je otvoreni standarizovani jezik zasnovan na XML-u, dizajniran za iskazivanje sigurnosnih propisa i prava pristupa podacima u okviru web servisa i poslovnih sigurnosnih aplikacija. Potvrđen od strane Organizacije za unapređenje uređenih informacionih standarda (OASIS - Organization for the Advancement of Structured Information Standards) u Februaru 2003 godine, XACML je razvijen s ciljem standarizovanja kontrole pristupa upotrebom XML-a, tako da npr. korisnik može pristupiti nekoliko uvezanih web sajtova samo jednom prijavom. XACML se nekad oslovljava i kao XACL (Extensible Access Control Language).

XACML je dizajniran tako da funkcioniše u kombinaciji sa SAML-om (Security Assertion Markup Language), drugim OASIS standardom. SAML definiše načine dijeljenja autorizacionih podataka, kao što su korisničke lozinke i bezbijednosne provjere, između sigurnosnih sistema. Komponenta za pravila (program koji ispituje ustanovljena pravila i predlaže ponašanje koje ide uz njih) zajedno sa propisima iskazanim u XCAML obliku, može porediti te informacije sa uspostavljenim kriterijumima kako bi se utvrdila prava korisnika. XACML specifikacija je razvijena zajedničkim naporima članica OASIS-a među kojima su IBM, Sun Microsystems i Entrust.

Uobičajena postavka je kada neko želi izvršiti neku akciju nad resursom. On će poslati zahtjev onome ko štiti taj resurs (kao što je fajl sistem ili web server), koga nazivamo PEP (Policy Enforcement Point). PEP će napraviti zahtjev na osnovu atribute naručioca, resursa koji se potražuju akcije koju želi izvršiti i ostalih informacija koje se odnose na zahtjev. PEP će zatim poslati to PDP-u (Policy Decision Point), koji će pogledati zahtjev i neke propise koji se odnose na njega, a zatim donijeti odluku da li pristup trebao biti odobren. Odgovor tj. odluka se vraća PEP-u, koji naručiocu može dozvoliti ili spriječiti pristup. PEP i PDP mogu biti dio jedne aplikacije ili raspoređeni na nekoliko servera.

Prednosti XACML-a:

* Standarizovan je. Upotrebom standarizovanog jezika, koristimo nešto što je provjereno od velikog broja stručnjaka i korisnika, te ne moramo svaki put praviti svoj sistem, razmišljati i nezgodnim problemima koji se pojavljuju pri stvaranju novog jezika. Uz to, kako XACML postaje sve rasprostranjeniji, sve je lakše upregnuti ga sa ostalim aplikacijama koje koriste isti standarizovani jezik.
* Generički je. To znači da umjesto pokušavanja obezbijeđivanja kotrole pristupa za neko određeno okruženje i posebnu vrstu resursa, može biti korišten u bilo kom okruženju. Jedan propis može biti zapisan a zatim se može koristiti u mnogim različitim vrstama aplikacija, i kada se koristi jedan zajednički jezik, upravljanje propisima postaje mnogo jednostavnije.
* Distribuisan je. To znači da propis može biti napisan tako da upućuje na druge propise koji se čuvaju na proizvoljnim lokacijama. Rezultat je da umjesto upravljanjem jednog monolitnog propisa, različite osobe ili grupe mogu po potrebi upravljati pod-elementima propisa, a XACML zna na koji način da kombinuje rezultate tih različitih propisa u jednu odluku.
* Moćan je. Dok postoje razni načini za proširenje osnovnog jezika, u većini okruženja neće biti potrebe za to. Standardni jezik već podržava širok spektar tipova podataka, funkcija i pravila o kombinovanju rezultata različitih propisa.

## Konstrukcije najvišeg nivoa: propisi (Policy) i skupovi propisa (PolicySet)

U korijenu svih XACML propisa je **propis** ili **skup propisa**. Skup propisa je spremište koje može sadržati druge propise ili skupove propisa, kao i reference (uputstva) prema propisima pronađenim u udaljenim lokacijama. **Propis** predstavlja jedan propis za kontrolu pristupa, izražen kroz skup **pravila** (**Rules**). Svaki XACML dokument propisa, sadrži tačno jedan korijenski XML tag propisa ili skupa propisa.

S obzirom na to da **propis** ili **skup propisa** može sadržati nekoliko propisa ili pravila, svaki od njih može dovesti to različitih odluka prava pristupa. XACML treba na neki način da uskladi svaku od odluka koje ti propisi donose. Ovo se vrši kroz kolekciju algoritama za kombinovanje (Combining Algorithms). Svaki algoritam predstavlja drugačiji način kombinovanja nekoliko odluka u jednu. Postoje algoritmi za kombinovanje propisa (Policy Combining Algorithm – koriste se od strane skupa propisa) i algoritmi za kombinovanje pravila (Rule Combining Algorithms – koriste se od strane propisa). Primjer jednog algoritma je algoritam – odbijanje nadglašava, koji kaže da bez obzira na sve, ako bilo koja procjena vrati status – odbijen (Deny), konačan rezultat je odbijanje. Ovi algoritmi za kombinovanje se koriste za izgradnju sve složenijih propisa, i dok postoji sedam standardnih algoritama kombinovanja, moguće je stvoriti i dodatne koji će odgovarati posebnim potrebama.

## Ciljevi (Targets) i pravila (Rules)

Dio zadatka XACML PDP-a je pronalaženje propisa koji se odnosi na upućeni zahtjev. Kako bi to izvršio, XACML obezbjeđuje još jednu karakteristiku pod nazivom **cilj** (**Target**). Cilj je u suštini skup pojednostavljenih uslova za subjekta, resurs i akciju koji moraju biti zadovoljeni kako bi se propis, skup propisa ili pravilo primijenili na dati zahtjev. Koriste funkcije istinitosti za poređenje vrijednosti pronađenih u zahtjevu sa onim koje se nalaze u cilju. Ako se zadovolje svi uslovi cilja, onda se propis, skup propisa ili pravilo koje je vezano za njega primjenjuje na zahtjev. Dodatno, da bi postajao način za provjeru primjenjivosti, cilj sadrži i informacije kojima se mogu označiti (indeksirati) propisi, što je korisno ukoliko će se čuvati veliki broj propisa a zatim vršiti brza pretraga kako bi se pronašli oni koji se odgovaraju. Npr. propis može sadržati cilj koji se odnosi samo na zahtjeve na određeni servis. Kada stigne zahtjev za pristup tom servisu, PDP će znati gdje da traži propise koji bi mogli odgovarati tom zahtjevu, zahvaljujući tome što su propisi označeni na osnovu ograničenja njihovih ciljeva. Cilj može biti označen i tako da je primjenjiv na bilo koji zahtjev.

Nakon što se propis pronađe i potvrdi da je odgovara zahtjevu, procjenjuju se njegova pravila. Propis može imati bilo koji broj pravila koja sadrže osnovnu logiku XACML propisa. Jezgro većine pravila je **uslov** (**Condition**), koji je funkcija tačnosti. Ako se uslov procijeni kao tačan, izvršiće se posljedica pravila. Procjena uslova može kao rezultat vratiti i grešku (Indeterminate) ili dovesti do zaključka da uslov nije primjenjiv na zahtjev (NotApplicable). Uslov može biti prilično složen, izgrađen od proizvoljnog broja ugnježdenih funkcija i atributa.

## Atributi (Attributes), vrijednosti atributa (Attribute Values) i funkcije (Functions)

Valuta kojom se XACML bavi su **atributi**. Atributi su imenovane vrijednosti poznatih tipova podatak koje mogu sadržati identifikator izdavaoca ili datum i vrijeme izdavanja. Atributi su karakteristike subjekta, resursa, akcije ili okruženja u kome je stvore zahtjev. Ime korisnika, njegova sigurnosna dozvola, datoteka kojoj želi pristupiti i trenutno vrijeme su atributske vrijednosti. Kada se zahtjev šalje od PEP-a prema PDP-u, on se sastoji gotovo isključivo od atributa koji će se kasnije porediti sa vrijednostima atributa u okviru propisa, kako bi se donijela odluka o dozvoli pristupa.

Propis razlučuje vrijednosti atributa iz zahtjeva ili iz nekog drugog izvora upotrebom dva mehanizma: **razvodnik atributa** (**AttributeDesignator**) i **odabirač atributa** (**AttributeSelector**). Razvodnik atributa dozvoljava propisu da naznači atribut sa određenim imenom i tipom, i eventualno i izdavačem, a zatim će PDP potražiti tu vrijednost u zahtjevu ili negdje drugo ukoliko je ne pronađe unutar zahtjeva. Postoje četiri vrste razvodnika, po jedan za svaku vrstu atributa u zahtjevu: **subjekat**, **resurs**, **akcija** i **okruženje**. Kako atribut subjekta može biti razdvojen u nekoliko različitih kategorija, **razvodnik atributa subjekta** (**SubjectAttributeDesignator**) može takođe navesti kategoriju u kojoj vršiti pretragu. Odabirač atributa dozvoljava propisu da pretražuje vrijednosti atributa kroz XPath upit. Tip podatka i XPath izraz se mogu koristiti za razriješavanje jednog skupa vrijednosti, bilo to u okviru zahtjeva ili negdje drugo.

I razvodnik i odabirač atributa moguu vratiti nekoliko vrijednosti (s obizirom na to da može postojati više poklapanja u zahtjevu), zbog čega XACML obezbjeđuje poseban atribut nazvan torba (Bag). Torba je neuređeni skup koji dozvoljava pojavu duplikata, te predstavlja ono što razvodnici i odabirači uvijek vraćaju, lak i se samo jedna vrijednost poklapa. U slučaju da nema poklapanja, vraća se prazna torba, iako razvodnik ili odabirač može postaviti oznaku koja u tom slučaju dovodi do greške umjesto vraćanja prazne torbe.

Nakon što se dopremi torba atributskih vrijednosti, treba ih analizirati na neki način kako bi se donije odluke o dozvoli za pristup. To se vrši kroz moćni sistem funkcija. Funkcije mogu raditi sa bilo kojom kombinacijom atributa, te mogu vratiti bilo koji tip vrijednosti atributa koji sistem podržava. Fnkcije takođe mogu biti ugnježdene, tako da je moguće imati funkcije koje operišu sa rezultatom druge funkcije, i ta hijerarhija može biti proizvoljne složenosti. Moguće je definisati prilagođene funkcije kako bi se obezbijedio još bogatiji jezik za izražavanje uslova pristupa.

Jedna napomena koju treba uzeti u obzir prilikom izgradnje ovih hijerarhija funkcija je to da većina funkcija radi sa određenim tipovima (kao što su nizovi karaktera ili cijeli brojevi) dok razvodnici i odabirači uvijek vraćaju torbe (Bags) vrijednosti. Kako bi to razriješio, XACML definiše skup standardnih funkcija koje prijamu torbu vrijednosti određenog tipa a zatim vraćaju jednu vrijednost tog tipa ukoliko se nalazi samo jedna vrijednost u torbi, ili grešku ukoliko se u torbi nalazi više ili ni jedna vrijednosti. To je jedna od funkcija koja se najčešće može vidjeti u okviru uslova. Takve funkcije nisu potrebne u ciljevima, pošto PDP automatski primjenjuje odgovarajuće funkcije svakom elementu torbe.

## Primjer jednog propisa

Navešćemo jedan jednostavan primjer **propisa** koristeći gore navedene osobine. Njegov **cilj** govori da se **propis** primjenjuje samo na zahtjeve prema serveru pod nazivom „UzorakServera“. **Propis** ima **pravilo** u okviru **cilja** koje zahtjeva akciju prijave i **uslov** koji se primjenjuje samo ako **subjekat** pokušava da se prijavi između 9:00 i 17:00. Ovaj primjer se može proširiti drugim **pravilima** za različite akcije. Ako prvo pravilo nije primjenjivo, biće primijenjeno podrazumijevano pravilo koje uvijek vraća odbijanje (Deny) (pravila se izvršavaju po redosledu).

<Policy PolicyId="SamplePolicy"

RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">

<!-- This Policy only applies to requests on the SampleServer -->

<Target>

<Subjects>

<AnySubject/>

</Subjects>

<Resources>

<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">SampleServer</AttributeValue>

<ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"

AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>

</ResourceMatch>

</Resources>

<Actions>

<AnyAction/>

</Actions>

</Target>

<!-- Rule to see if we should allow the Subject to login -->

<Rule RuleId="LoginRule" Effect="Permit">

<!-- Only use this Rule if the action is login -->

<Target>

<Subjects>

<AnySubject/>

</Subjects>

<Resources>

<AnyResource/>

</Resources>

<Actions>

<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">login</AttributeValue>

<ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"

AttributeId="ServerAction"/>

</ActionMatch>

</Actions>

</Target>

<!-- Only allow logins from 9am to 5pm -->

<Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than-or-equal"

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">

<EnvironmentAttributeSelector DataType="http://www.w3.org/2001/XMLSchema#time"

AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"/>

</Apply>

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">09:00:00</AttributeValue>

</Apply>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-less-than-or-equal"

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">

<EnvironmentAttributeSelector DataType="http://www.w3.org/2001/XMLSchema#time"

AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"/>

</Apply>

<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">17:00:00</AttributeValue>

</Apply>

</Condition>

</Rule>

<!-- We could include other Rules for different actions here -->

<!-- A final, "fall-through" Rule that always Denies -->

<Rule RuleId="FinalRule" Effect="Deny"/>

</Policy>

# 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.

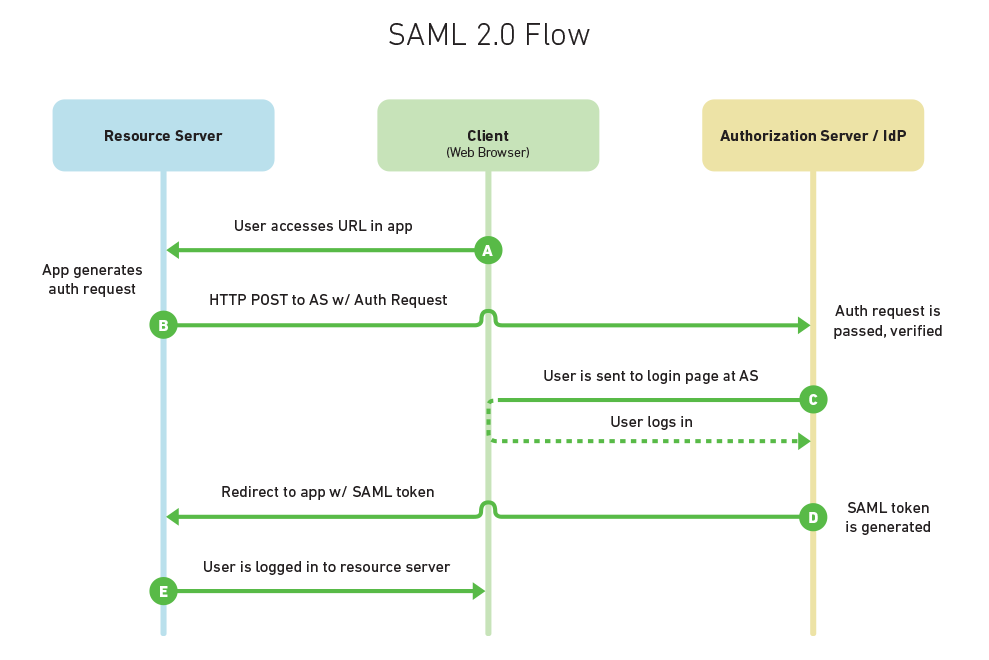
Kako bi se korisniku omogućilo takvo iskustvo, potrebno je implementirati SSO rješenje. Postoji mnogo strategija za implementaciju SSO-a, ali ćemo analizirati i porediti dvije najpopularnije – SAML i OAuth2.

## 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 - 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.

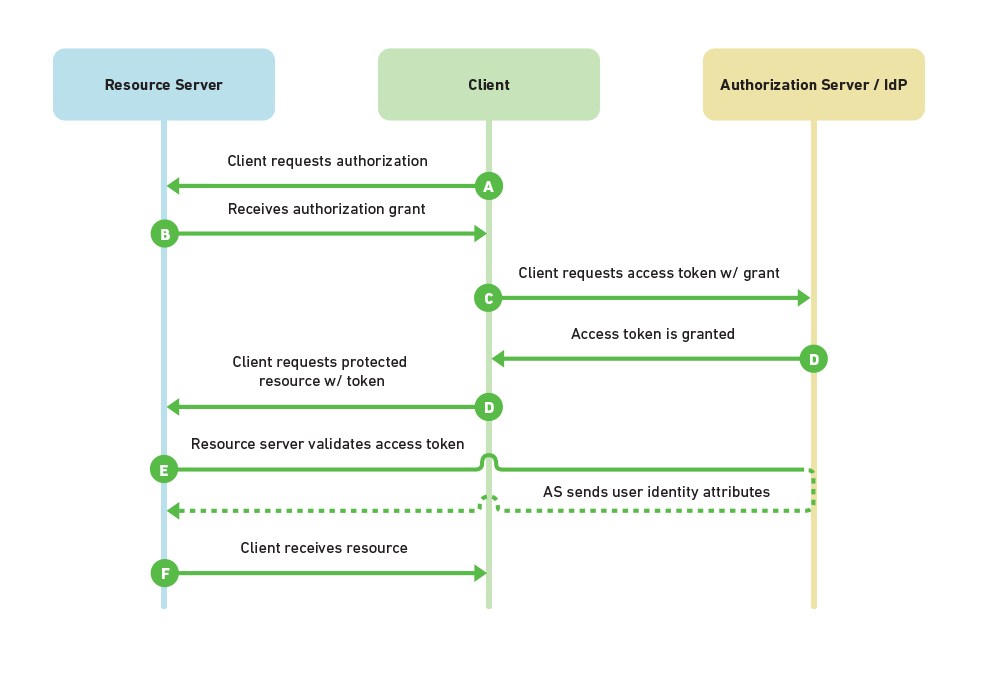
Mobilni uređaji i nativne aplikacije danas napreduju na način koji SAML nije mogao očekivati 2005. godine.

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 - 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.

## Konfigurisanje i pokretanje SP i IdP aplikacija

S obzirom da su u pitanju Spring Boot aplikacije, sama konfiguracija i pokretanje su veoma jednostavni. Pošto IdP koristi bazu za autorizaciju korisnika i izvlačenje rola, neophodno je da na računaru postoji SQL baza podataka. U okviru IdP projekta se nalaze skripte za inicijalizovanje baze (schema.sql) i popunjavanje tabela sa testnim podacima (data.sql). Potrebno je izvršiti naredne korake:

1. Raspakovati **sso-project.zip** na zeljenu lokaciju na disku ili odraditi checkout projekta sa GitHub repozitorija - <https://github.com/racog3/sso-project.git>
2. Otvoriti direktorij pod nazivom **IdentificationProvider** i podesiti **application.properties** fajl tako da **spring.datasource** parametri imaju ispravne postavke za povezivanje na bazu podataka.
3. Izvršiti Maven komandu – **mvn clean install**. Ovim korakom će se izvršiti i pakovanje neophodne klijentske biblioteke 'IdentificationProvider-x.x-client.jar' te njeno instaliranje u lokalni maven repozitorij kako bi se mogla koristiti kao *dependency* u okviru klijentski aplikacija SP1 i SP2.
4. Otvoriti i direktorije pod nazivima '**ServiceProvider**' i '**ServiceProvider2**' i u okviru njih takodje izvršiti **mvn clean install** komandu.
5. Pokrenuti SSO server pokretanjem main aplikacije u okviru **IdentificationProvider** projekta.
6. Pokrenuti klijentske demo aplikacije u okviru **ServiceProvider** i **ServiceProvider2** projekata.

Unutar **application.properties** fajlova u okviru sve tri aplikacije, promjenom **server.context** i **server.port** parametara moguće je prilagoditi kontekst i port na kom će server uslužiti aplikaciju. Za klijentske aplikacije je moguće podesiti putanju koja će vršiti obradu SAML odgovora, a trenutno je postavljena na **/saml**.

**Napomena:** Paziti da je u okviru **application.properties** fajlova koji se nalaze u klijentskim aplikacijama ispravno podešena adresa IdP-a tj SSO servera – **sso.idp.address**

Podrazumijevane adrese pri lokalnom pokretanju aplikacija:

SP1 - <http://localhost:8081/sp1>

SP2 - <http://localhost:8082/sp2>

IdP (SSO) – http://localhost:8080/sso/

Predefinisani tesni korisnici u data.sql skripti:

1. Korisnik 1

username: [user1@etfbl.net](mailto:user1@etfbl.net)

password: 1234

Ima pristup zaštićenoj stranici na obije klijentske aplikacije:

<http://localhost:8081/sp1/protectedResource>

<http://localhost:8082/sp2/protectedResource>

1. Korisnik 2

username: [user2@etfbl.net](mailto:user2@etfbl.net)

password: 1234

Ima pristup zaštićenoj stranici na drugoj klijentskoj aplikaciji:

<http://localhost:8082/sp2/protectedResource>

ali nema pristup žaštićenoj stranici na prvoj klijentskoj aplikaciji:

<http://localhost:8081/sp1/protectedResource>