# Sustav jedinstvene autentikacije korisnika (SSO)

Sustav jedinstvene autentikacije korisnika (engl. single Sign-On, SSO) je autentikacijski mehanizam koji omogućuje da se korisnik u sustav prijavi samo jednom i nakon toga pristupa svim aplikacijama koje koriste SSO servis bez potrebe za ponovnim unosom korisničke oznake i zaporke.

Uporaba Single sign-On servisa znatno poboljšava doživljaj korisnika prilikom prijavljivanja u veći broj aplikacija, jer za prijavu u sve aplikacije korisnik rabi isti elektronički identitet.



## Prednosti SSO autentikacije

Za korisnike:

- manji broj vjerodajnica (korisničkih imena i zaporki) za zapamtiti
- manji broj autentikacijskih događaja prilikom pristupa uslugama (manji broj unosa vjerodajnica)
- pristup različitim uslugama pomoću istih vjerodajnica

Za davatelje usluga:

- delegiranje dijela poslova oko implementacije autentikacije (npr. implementacija ekrana za prijavu, validacija vjerodajnica, autentikacija korisnika, sigurno čuvanje korisničkih podataka i sl.)
- implementacija autentikacije po standardnim autentikacijskim protokolima
- korištenje različitih načina autentikacije korisnika (korisničko ime i zaporka, višestupanjska autentikacija...)

Sigurnosni aspekti:

- nema izlaganja korisničkih vjerodajnica usluzi kojoj korisnik želi pristupiti (autentikacija se događa kod davatelja elektroničkog identiteta)

## Elektronički identitet

Identitet definiramo kao skup atributa (podataka) o pojedincu tj. ljudskoj osobi. Identitet može sadržavati podatke kao što su ime i prezime osobe, adresa prebivališta i slično.

Uz općenite atribute koji opisuju osobu, svaki identitet sadrži i neki atribut koji jedinstveno određuje osobu u nekom kontekstu. Takav atribut nazivamo identifikatorom. Neki primjeri identifikatora su OIB, JMBAG, broj osobne iskaznice, broj putovnice ili slično. Identifikatori imaju vrlo značajnu ulogu u sustavima za upravljanje identitetima te u postupcima autentikacije osobe.

> Ako su podaci o identitetu dostupni u elektroničkom obliku, onda govorimo o elektroničkom identitetu.

U sustavu AAI@EduHr, elektronički identiteti nastaju na matičnim ustanovama, a spremljeni su u LDAP imenicima.

> Jedna osoba može imati više elektroničkih identiteta u različitim kontekstima. Na primjer, osoba može imati elektronički identitet u sustavu NIAS (nacionalni identifikacijski i autentikacijski sustav), u sustavu AAI@EduHr (identifikacijski i autentikacijski sustav znanosti i obrazovanja), te u bilo kojem drugom sustavu koji posjeduje podatke o osobi i nudi funkcionalnosti identifikacije i autentikacije.

### eduHr shema

U sustavu AAI@EduHr, atributi koji su dostupni o nekoj osobi definirani su eduHr shemom. To znači da su atributi propisani, tj. da imaju određenu semantiku i sintaksu. To olakšava njihovo korištenje jer davatelji usluga znaju koje podatke (i u kojem obliku) mogu očekivati o osobi.

### Elektronički identitet naspram korisničkih računa

Pojam "elektronički identitet" se ponekad zna pomiješati s pojmom "korisnički račun" (engl. account). Korisnički račun osobe tipično se odnosi na *konst rukciju* u nekoj usluzi tj. nekom informacijskom sustavu, servisu ili aplikaciji pomoću koje osoba obavlja radnje u samom sustavu / servisu / aplikaciji. Korisnički račun često sadrži podatke o osobi koji su preuzeti iz samog identiteta osobe, a tipično sadrži i dodatne podatke i identifikator(e) relevantne za sam sustav / servis / aplikaciju. Dakle, generalno govoreći, osoba će koristiti elektronički identitet prilikom autentikacije u uslugu, a usluga će osobu autorizirati te kreirati lokalni korisnički račun za obavljanje radnji u usluzi.

> Općenito govoreći, osim za osobe, identitet može biti vezan i za druge entitete kao što su uređaji, programski klijenti i slično. Na primjer, identitet za neki uređaj može sadržavati podatke kao što su naziv uređaja, model, verziju firmware-a, neki identifikator kao što je neki nasumičan ID, IP adresa i slično. U određenim autentikacijskim protokolima predviđeno je i da takvi entiteti mogu obavljati postupke autentikacije na sličan način kao i osobe. U sustavu AAI@EduHr, elektronički identitet je uvijek vezan za osobu (student, učenik, zaposlenici na ustanovama) te postupak autentikacije obavlja sama osoba, tj. vlasnik elektroničkog identiteta (krajnji korisnik).

# Federacija identiteta

Sustav AAI@EduHr često nazivamo federacijom identiteta u sustavu znanosti i obrazovanja, ili skraćeno AAI@EduHr federacijom.

Općenito govoreći, federacija identiteta (ili samo federacija) je skup organizacija koje dogovorno surađuju prema određenom skupu pravila. Pravila se obično sastoje od pravnih okvira, politika, tehničkih profila i standarda. U sklopu federacije, jedna od organizacija tipično ima i ulogu koordinatora federacije, što znači da ona koordinira, održava i razvija sustav na tehničkoj i operativnoj razini.  Svrha federacije je uspostava povjerenja između različitih dionika federacije te osiguravanje sigurne razmjene podataka o identitetu prilikom pristupa uslugama (autentikacije) unutar federacije.

> Ustroj AAI@EduHr federacije reguliran je Pravilnikom, a poslove koordinacije, razvoja i održavanja sustava AAI@EduHr obavlja Srce - Sveučilišni računski centar Sveučilišta u Zagrebu.

## Elementi federacije

Tipična federacija identiteta se sastoji od konceptualnih elemenata kao što su davatelji elektroničkih identiteta, davatelji usluga te krajnji korisnici koji koriste dostupne usluge temeljem svojeg elektroničkog identiteta.

Elementi AAI@EduHr federacije su:

- matične ustanove - davatelji elektroničkih identiteta, npr. sveučilišta, fakulteti, visoke škole, škole, znanstvene ustanove
- krajnji korisnici - vlasnici elektroničkog identiteta, npr. profesori, studenti, učenici, zaposlenici na ustanovi
- davatelji usluga (resursa) - matične ustanove ili partneri
- središnji AAI@EduHr servisi - posrednički sustav između korisnika, usluge i matične ustanove koji se koristi prilikom postupka autentikacije

Dakle, matične ustanove u AAI@EduHr federaciji, uz ulogu davatelja elektroničkih identiteta, mogu imati i ulogu davatelja usluge. S druge strane, partneri AAI@EduHr federacije mogu imati samo ulogu davatelja usluge. Na primjer, partneri mogu biti komercijalne tvrtke koje nude usluge korisnicima u sustavu znanosti i obrazovanja.

## Granice federacije

Tipičan način uspostave federacije identiteta u sustavima znanosti i obrazovanja (akademske federacije) je uspostava na nacionalnoj razini. Dakle, aka demske federacije identiteta tipično djeluju unutar granica jedne države, pa se često nazivaju i nacionalnim akademskim federacijama.

Uz nacionalne federacije postoje i interfederacijski servisi koji omogućuju povezivanje postojećih nacionalnih federacija u konfederaciju. Članovi konfederacije (slično kao i članovi nacionalnih federacija) dogovorno surađuju na temelju skupa pravila i standarda koji osiguravaju interoperabilnost. Svrha konfederacije je osiguravanje pouzdane razmjene podataka vezanih uz identitet između federacija članica.

Jedan od takvih interfederacijskih servisa je eduGAIN, a cilj mu je omogućiti funkcionalnosti jedinstvene autentikacije na europskoj i globalnoj razini za članove akademske zajednice.

> AAI@EduHr je punopravna članica eduGAIN-a od lipnja 2011. godine.

## Tipovi arhitekture federacije

Gledano kroz arhitekturu, federacije identiteta se obično dijele na *mesh* i *hub-and-spoke* tipove.

### *Mesh* arhitektura federacije

*Mesh* arhitektura je arhitektura u kojoj su sve komponente distribuirane na svakoj ustanovi koja sudjeluje u federaciji. Nema centralnog servisa koji prima autentikacijske zahtjeve i odgovara na njih, nego svaka ustanova ima svoj servis koji obavlja tu zadaću (uloga davatelja identiteta). Uz to, svaka ustanova može imati usluge koje pruža. Svi ti entiteti (davatelji identiteta i usluga) su popisani u katalogu (u SAML-u to je XML s metapodacima davatelja) koji je dostupan svim dionicima federacije. Dakle, taj katalog govori tko je tko u federaciji i koje funkcionalnosti pruža. Glavni izazov u *mesh* f ederacijama je upravljanje metapodacima i uspostava povjerenja svih entiteta u federaciji, određivanje koji atributi o osobi će biti dostupni kojim uslugama, te implementacija novih autentikacijskih protokola.

### *Hub-and-spoke* arhitektura federacije

*Hub-and-spoke* tip arhitekture federacije se može implementirati na dva načina.

Prvi način je da se implementira središnji *proxy* servis koji sluša na autentikacijske zahtjeve i prosljeđuje ih autentikacijskom servisu na određenoj ustanovi na obradu. Po vraćanju odgovora s autentikacijskog servisa na ustanovi, *proxy* prosljeđuje odgovor originalnom zahtjevatelju. Dakle, svaka ustanova i dalje ima servis koji obrađuje autentikacijske zahtjeve, samo što zahtjeve ne dobiva od različitih usluga, nego ih šalje, tj. prosljeđuje središnji *proxy*. Zbog toga, servisi za autentikaciju na ustanovama (davatelji identiteta) moraju znati jedino za središnji *proxy*, jer jedino će od njega dobivati autentikacijske zahtjeve. S druge strane, davatelji usluga moraju znati jedino za središnji *proxy*, jer jedino će njemu slati autentikacijske zahtjeve. Dakle, postojanje središnjeg *proxy-a* donekle pojednostavljuje uspostavu povjerenja. Nedostatak ovog tipa arhitekture je da ako se dogodi kvar na *proxy-u,* čitava federacija prestaje s radom. Drugi nedostatak je da je implementacija novih autentikacijskih protokola i dalje kompliciranа jer ih je potrebno implementirati na autentikacijskom servisu svih ustanova (davateljima identiteta). Prednost ovog tipa arhitekture je da korisnik unosi svoje vjerodajnice direktno na servisu svoje matične ustanove, a s druge strane *proxy* može kontrolirati koji atributi o osobi će biti dostupni uslugama te ih može po potrebi transformirati.

Drugi način implementacije *hub-and-spoke* arhitekture je implementacija središnjeg autentikacijskog servisa koji ima neki oblik pristupa bazi elektroničkih identiteta na ustanovi.  U ovom tipu arhitekture ustanove nemaju servis koji obrađuje autentikacijske zahtjeve, što implementaciju čini jednostavnijom. Korisnici unose svoje vjerodajnice na centralnom autentikacijskom servisu koji onda na neki način obavlja provjeru vjerodajnica na samoj ustanovi. Nedostatak ovog tipa arhitekture je da ako se dogodi kvar na centralnom autentikacijskom servisu, čitava federacija prestaje s radom. Prednost ovog tipa arhitekture je da centralni autentikacijski servis predstavlja jedno mjesto uspostave povjerenja, te je implementacija novih autentikacijskih protokola jednostavnija (mora se implementirati samo na jednom mjestu, na centralnom autentikacijskom servisu).

> Arhitektura federacije AAI@EduHr je *hub-and-spoke* s centralnim autentikacijskim servisom, a komunikacija s bazom elektroničkih identiteta na ustanovi obavlja se HTTPS / SOAP protokolom.

## Federacijski protokoli

Tehnički gledano, funkcioniranje federacije se temelji na korištenju otvorenih tehnologija, standarda, specifikacija i protokola. Koristeći otvorene tehnologije svi dionici federacije mogu postići interoperabilnost, povjerenje i ciljanu sigurnost.

Jedna od najpopularnijih tehnologija za uspostavu i funkcioniranje federacija je Security Assertion Markup Language (SAML). Protokol SAML je začetnik u definiranju i popularizaciji entiteta kao što su "davatelj identiteta" (engl. identity provider), davatelj usluge (engl. service provider), te u definiranju na koji način ostvariti povjerenje između njih razmjenom strukturiranih metapodataka. Uz to, definira i na koji način omogućiti jedinstvenu autentikaciju (engl. Single Sign-On, SSO) krajnjeg korisnika na uslugama, tj. definira siguran način isporuke autentikacijskih i autorizacijskih atributa krajnjeg korisnika samoj usluzi. Pri tome davatelj identiteta i davatelj usluge mogu biti na različitim domenama.

Uz SAML, neki od drugih protokola za uspostavu i funkcioniranje federacija su obitelj protokola OpenID i WS-Federation.

## Usuglašavanje identifikatora za identitet

Bitna zadaća federacijskih protokola je omogućavanje da se različiti entiteti u federaciji usuglase oko toga koji atribut u elektroničkom identitetu će se koristiti kao identifikator, te u kojem formatu. Federacijski protokoli tipično omogućuju dva načina definiranja identifikatora:

- isti identifikator za različite usluge (različite usluge mogu povezati iste korisnike) - na primjer, OIB ili slično.
- različit identifikator za različite usluge (različite usluge ne mogu povezati iste korisnike) - formira se za svaku uslugu zasebno. Na primjer, to može biti *hash* vrijednost konkateniranih vrijednosti nekog identifikatora iz identiteta i identifikatora same usluge.

Usuglašavanje se obavlja razmjenom metapodataka između davatelja identiteta i davatelja usluga, pri čemu se, između ostalog, konfigurira koji atribut i u kojem formatu će se koristiti kao identifikator. Tako isti davatelj identiteta može za različite usluge vraćati različite ili iste identifikatore za istu osobu, ovisno o konfiguraciji.

Uz predodređeni identifikator konfiguriran u metapodacima, federacijski protokoli tipično omogućuju i da usluga bira koji identifikator i u kojem obliku želi (dinamičko definiranje identifikatora) prilikom samog autentikacijskog postupka.

## Povjerenje i kriptografija

Federacijski protokoli tipično koriste funkcionalnosti iz kriptografije javnog ključa (engl. public key cryptography) za potpisivanje autentikacijskih poruka i dokumenata (dokumenti mogu biti npr. metapodaci različitih entiteta u federaciji). Svrha korištenja kriptografije može biti zaštita podataka šifriranjem (kriptiranje, engl. encryption) ili verifikacija podataka pomoću digitalnog potpisa. Javni ključevi entiteta će tipično biti dostupni u metapodacima samih entiteta. Na primjer, davatelj identiteta će objaviti svoj javni ključ u svojim metapodacima, a davatelj usluge u svojim. Tako različiti entiteti mogu koristiti javne ključeve za šifriranje autentikacijskih poruka.

Kada su javni ključevi razmijenjeni, davatelj usluge može koristiti javni ključ od davatelja identiteta za šifriranje autentikacijskog zahtjeva kojeg šalje prema davatelju identiteta, a davatelj identiteta će onda koristiti svoj privatni ključ za dešifriranje autentikacijskog zahtjeva. Nakon toga, davatelj identiteta može autentikacijski odgovor šifrirati javnim ključem od davatelja usluge te ga poslati samoj usluzi. Davatelj usluge će onda koristiti svoj privatni ključ za dešifriranje autentikacijskog odgovora.

Uz šifriranje, autentikacijske poruke mogu biti i digitalno potpisane. Na primjer, davatelj usluge može digitalno potpisati autentikacijski zahtjev svojim privatnim ključem, a davatelj identiteta takav potpis može onda provjeriti pomoću javnog ključa od davatelja usluge. Nakon toga, davatelj identiteta može potpisati autentikacijski odgovor svojim privatnim ključem, a davatelj usluge takav potpis onda može provjeriti pomoću javnog ključa od davatelja identiteta.

Uz potpisivanje autentikacijskih poruka, često se obavlja i potpisivanje metapodataka samih entiteta, čime se omogućuje provjera ispravnosti i izvornosti samih metapodataka. Na primjer, davatelj identiteta može potpisati svoje metapodatke svojim privatnim ključem, a davatelj usluge onda može provjeriti takav potpis pomoću javnog ključa davatelja identiteta.

# Autentikacija naspram autorizacije

Općenito govoreći, da bi osoba mogla pristupiti nekoj usluzi obično se mora autenticirati. Prilikom autentikacije, osoba unosi svoje vjerodajnice npr. korisničku oznaku i zaporku (ili dodatni podatak u slučaju dodatnog ili jačeg autentikacijskog mehanizma). Unesene vjerodajnice se provjeravaju u odnosu na prethodno registrirane podatke. Ako podaci odgovaraju, korisnik je autenticiran.

Nakon autentikacije, usluga tipično koristi (ili otvara) lokalni korisnički račun za osobu te obavlja postupak autorizacije kojim se definira što osoba može raditi u usluzi, odnosno koje privilegije osoba ima. Autorizacija se može obaviti na temelju podataka iz samog elektroničkog identiteta osobe ili se definira po korisničkom računu, ulozi u usluzi ili slično.

## Jačina autentikacije

Postoje različiti načini autenticiranja korisnika, a svaki od njih govori o tome koliko je sigurno da je osoba koja je obavila autentikaciju stvarni vlasnik elektroničkog identiteta kojim se osoba predstavila prilikom autentikacije.

Trenutno najrasprostranjeniji način autenticiranja korisnika je pomoću vjerodajnica u obliku korisničkog imena i zaporke. Ovaj način se smatra slabijim načinom autentikacije jer sa sobom nosi nižu razinu sigurnosti u odnosu na ostale autentikacijske mehanizme. Razlozi za nisku razinu sigurnosti proizlaze iz poznatih boljki rada sa zaporkama. Na primjer, ako se koristi prekratka zaporka, relativno lako ju je pogoditi. Kada se koristi preduga zaporka, korisnici ju često znaju negdje zapisati, pa ju je moguće lakše ukrasti. Ako dođe do krađe zaporke, korisnici često toga nisu svjesni (teško je primijetiti da je zaporka ukradena).

Jači načini autentikacije tipično koriste tehnologije kao što su

- jednokratne zaporke (one-time password, OTP)
- asimetrična kriptografija (par privatnog i javnog kriptografskog ključa)
- biometrijske tehnologije

Pri korištenju jednokratne zaporke, OTP se, na neki način, generira prilikom same autentikacije. OTP je moguće iskoristiti samo jednom, pa ga je teže ukrasti i iskoristiti. Na primjer, prilikom autentikacije OTP se može korisniku poslati na e-mail, ili korisnik može generirati OTP na prethodno registriranom uređaju ili mobilnoj aplikaciji. Korisnik unosi OTP u formu za autentikaciju i tako potvrđuje svoj identitet.

Pri korištenju asimetrične kriptografije u postupku autentikacije, korisnik može imati privatni ključ spremljen na nekom uređaju (USB ključ, mobitel), pametnoj kartici ili slično. Prilikom autentikacije, korisnik može potpisati autentikacijski zahtjev svojim privatnim ključem, a autentikacijski servis može provjeriti taj potpis pomoću korisnikovog javnog ključa i tako potvrditi korisnikov identitet. Sam postupak potpisivanja se može odraditi tako da korisnik npr. unese PIN na uređaju, klikne određeni gumbić ili slično.

Korištenje biometrijskih tehnologija kao što je (prepoznavanje otiska prsta, skeniranje lica ili oka) znači i visoku pouzdanost autentikacije, ali ima jednu manu. Naime, iako se to relativno rijetko događa, potrebno je imati na umu da u slučaju oštećenja ili gubitka biometrijskog elementa korištenog pri autentikaciji, njega više nije moguće npr. ponovno izdati kao što je to moguće u drugim mehanizmima autentikacije. Dakle, u takvim slučajevima često se obavlja prijenos na drugi način autentikacije, ili eventualno registracija drugog biometrijskog elementa za autentikaciju.

## Višestupanjska autentikacija

Drugi način povećavanja sigurnosti autentikacije je korištenje višestupanjske autentikacije (MFA, Multi-Factor Authentication) u kojoj je korisnik autenticiran nakon što se uspješno autenticira kombinacijom dvije ili više metoda autentikacije. Pri tome se može kombinirati autentikacija pomoću onoga što korisnik zna (npr. korisnička oznaka i zaporka) s autentikacijom putem onog što korisnik ima (npr. uređaj za generiranje OTP-a, pametna kartica) i/ili s autentikacijom putem korisnikovih biometrijskih podataka (npr. otisak prsta).

Sustav AAI@EduHr omogućava dvostupanjsku autentikaciju tako da se kao prvi stupanj koristi metoda autentikacije korisničkom oznakom i zaporkom, a kao drugi stupanj neki od sustava koji generira jednokratne zaporke (tokene).

# Jedinstvena autentikacija (engl. Single Sign-On - SSO)

Jedna od funkcionalnosti koju definiraju federacijski protokoli je jedinstvena autentikacija (engl. Single Sigh-On - SSO). Jedinstvena autentikacija znači da se krajnji korisnik autenticira samo jednom (u nekom periodu), a nakon toga pristupa različitim uslugama na različitim domenama bez potrebe za ponovnom autentikacijom.

Da bi jedinstvena autentikacija funkcionirala između različitih usluga, usluge moraju delegirati autentikaciju istom autentikacijskom servisu. Na primjer, usluga *A* dostupna na *https://usluga-a.primjer* i usluga *B* dostupna na *https://usluga-b.primjer* delegiraju autentikaciju davatelju identiteta *C* dostupnom na *https://davatelj-identiteta.primjer*. Ako korisnik pokuša pristupiti usluzi A, ona će ga preusmjeriti na autentikaciju na davatelja identiteta C na autentikaciju. Nakon uspješne autentikacije na davatelju identiteta, korisnik sada može pristupati i drugim uslugama, dakle i usluzi B, bez potrebe za ponovnom autentikacijom.

Jedinstvena autentikacija u sustavu AAI@EduHr može se obaviti preko protokola

- Security Assertion Markup Language (SAML) 2.0
- OpenID Connect (OIDC)
- Central Authentication Service (CAS)

## SSO sjednica

Generalno govoreći, nakon što se osoba autenticira u nekom sustavu, za nju se tipično otvara tzv. sjednica (engl. session). Pomoću sjednice sustav može pratiti je li korisnik autenticiran, kada se autenticirao, te neke druge podatke kao što je korisnička oznaka i slično. Tako sustav ne mora za svaku radnju tražiti ponovnu autentikaciju i podatke iz identiteta. Uz to, sustav tipično ima postavljeno ograničenje trajanja sjednice, pa u slučaju isteka sjednice može tražiti korisnika ponovnu autentikaciju. Istek sjednice tj. ponovna autentikacija se obavlja kako bi se provjerilo da je "za ekranom" još uvijek ista osoba koja se prethodno prijavila. Trajanje sjednice se razlikuje od sustava do sustava, a oblično ovisi o osjetljivosti radnji koje je moguće obaviti u sustavu. Na primjer, sustavi on-line bankarstva će tipično imati vrlo kratku sjednicu, na primjer trajanja nekoliko minuta, dok će neki drugi manje osjetljivi sustavi imati sjednicu od nekoliko sati, dana ili dulje.

U slučaju obavljanja jedinstvene autentikacije korisnika, tipično će postojati bar dva mjesta na kojima će se otvoriti korisnička sjednica. Jedna će biti otvorena na samoj usluzi (ili više usluga ako korisnik pristupi više usluga), a druga na strani davatelja identiteta tj. na strani autentikacijskog servisa. Sjednica na strani autentikacijskog servisa se naziva SSO sjednica i ona je razlog zašto korisnik ne mora ponovno unositi vjerodajnice nakon što se prvi put autenticira na autentikacijskom servisu (u nekom periodu). Uz vođenje same SSO sjednice, autentikacijski servis će tipično voditi i evidenciju o tome na kojim sve uslugama korisnik ima otvorenu sjednicu.

Funkcionalnost SSO sjednica realizirana je kroz standardno korištenje kolačića (engl. cookies) u web preglednicima.

U sustavu AAI@EduHr trajanje sjednice je 8 sati. To znači da se osoba, nakon što se prvi put prijavi u sustav AAI@EduHr, ne mora ponovno prijavljivati sljedećih 8 sati.

## Uloga web preglednika u SSO

U federacijskim protokolima tipično se koristi web preglednik za obavljanje jedinstvene autentikacije, a razloga za to je više.

Prva funkcionalnost web preglednika koja se koristi prilikom jedinstvene autentikacije je HTTP preusmjeravanje. Pomoću HTTP preusmjeravanja u web pregledniku, davatelj usluge može krajnjeg korisnika preusmjeriti na autentikacijski servis davatelja identiteta, a davatelj identiteta onda može, nakon autentikacije, preusmjeriti korisnika natrag na davatelja usluge.

Drugo, uloga web preglednika je i realizacija funkcionalnosti SSO sjednice pomoću kolačića.

Treće, uloga web preglednika je i da služi kao neovisna aplikacija u koju krajnji korisnik unosi svoje vjerodajnice (npr. korisničko ime i zaporku, ili neki drugi oblik vjerodajnica), te da služi za prijenos korisničkih atributa između davatelja identiteta i davatelja usluge. Naime, čak i ako su usluge realizirane kao nativne aplikacije (npr. mobilne aplikacije), uvijek će se koristiti web preglednik za unos vjerodajnica i slanje autentikacijskih poruka i odgovora. Time se osigurava da korisnik ne unosi vjerodajnice u aplikaciju nad kojom kontrolu ima samo davatelj usluge, tj. osigurava se da korisnik unosi vjerodajnice samo na strani davatelja identiteta.

## Izazovi s kolačićima u SSO

Jedna od svrha korištenja kolačića u HTTP komunikaciji između web preglednika i nekog servera je očuvanje stanja (engl. state) između različitih HTTP zahtjeva (HTTP protokol je inače *stateless*). Tako se mogu voditi korisničke sjednice na serveru, odnosno provjeriti je li korisnik autenticiran ili slično. Druga svrha korištenja kolačića spremanje korisničkih podataka ili postavki. Na primjer, kolačići se mogu koristiti za spremanje naznake prihvaćanja uvjeta korištenja usluge, ili spremanje postavka jezika sučelja usluge, ili slično.

Treći, sve više problematičan način korištenja kolačića je praćenje korisnika na internetu u svrhu, npr. prikazivanja prilagođenih reklama. Naime, praćenjem navika korisnika prilikom surfanja na internetu, te praćenjem sadržaja kojeg korisnik konzumira, korisniku je moguće prikazati ciljane reklame, tj. one koje bi ga mogle najviše interesirati.

Kako bi se zaštitila privatnost korisnika, donesene su regulative (GDPR, ili ranije ePrivacy Directive (EPD)) koje definiraju kada i u koju svrhu se kolačići mogu koristiti, te nužnost informiranja korisnika o korištenju kolačića. Rezultat je da korisnik treba dati suglasnost za korištenje kolačića, a iznimno usluga može koristiti kolačiće i kada ima legitimni interes.

Uz regulative koje definiraju način korištenja kolačića, proizvođači web preglednika su počeli implementirati tehničke restrikcije u svrhu bolje početne zaštite privatnosti korisnika na internetu. Jedna od takvih zaštita je korištenje atributa SameSite koji određuje u kojem kontekstu će se kolačići moći razmjenjivati između servera i web pregledanika u komunikaciji između različitih domena.

Pošto se vođenje SSO sjednice oslanja na funkcionalnost korištenja kolačića između različitih domena (davatelj identiteta i davatelj usluge su na različitim domenama), atribut kolačića SameSite ima direktan utjecaj na obavljanje postupka jedinstvene autentikacije. Stoga, prilikom konfiguriranja davatelja identiteta ali i same usluge, potrebno je voditi računa da se na ispravan način podesi atribut kolačića SameSite.

### Dijagram obavljanja SSO autentikacije na primjeru sustava AAI@EduHr (video)

Your browser does not support the HTML5 video element

Kratki opis postupka:

- oblak davatelja usluga se odnosi na više različitih usluga. Korisnik prvo pristupa jednoj usluzi (na kojoj nije lokalno autenticiran), a koja preusmjerava na autentikaciju na AAI@EduHr autentikacijski servis. Za preusmjeravanje se koristi web preglednik, neovisno radi li se o usluzi realiziranoj kao web aplikacija ili kao nativna aplikacijama (na nativnim aplikacijama će se podignuti sistemski web preglednik). Efektivno se šalje određeni HTTP zahtjev na određeni URL na središnjim autentikacijskim servisima po SSO protokolu
- središnji autentikacijski servis provjerava je li korisnik već autenticiran. U ovom slučaju nije, stoga se obavlja preusmjeravanje na autentikaciju na određeni URL na središnjem servisu. Pritom se kreira i korisnička sjednica te se postavlja kolačić koji sadrži identifikator SSO sjednice
- na autentikacijskom URL-u na središnjem servisu korisnik unosi vjerodajnice. Nakon toga, u slučaju AAI@EduHr federacije, u pozadini se koristi AOSI Web Service (WS) na korisnikovoj matičnoj ustanovi za autentikaciju i dohvat atributa. Po uspješnoj autentikaciji, usluzi se vraćaju korisnički atributi.
- kada korisnik pristupi drugoj usluzi na kojoj nije lokalno autenticiran, također se obavlja preusmjeravanje na središnji autentikacijski servis. No, ovaj put web preglednik će ujedno poslati i kolačić koji sadrži ID SSO sjednice. Središnji servisi će provjeriti valjanost sjednice, dohvatiti korisničke podatke iz *cache-a*, te odmah vratiti autentikacijski odgovor usluzi (korisnik se nije trebao ponovno autenticirati).

## Jedinstvena odjava (engl. Single Logout - SLO)

Uz jedinstvenu autentikaciju, federacijski protokoli tipično omogućuju i jedinstvenu odjavu (SLO), dakle odjavu korisnika sa autentikacijskog servisa i sa usluga. Pošto sjednice postoje na više mjesta (na autentikacijskom servisu i uslugama), prvo treba odlučiti što se uopće treba dogoditi u kojem scenariju. Na primjer, treba li se dogoditi jedinstvena odjava ako istekne sjednica na nekoj usluzi ili samo ako korisnik sam inicira odjavu npr. klikom na gumb za odjavu? Treba li se ukidanjem sjednice na usluzi ukinuti i SSO sjednica na autentikacijskom servisu?

Ako se treba dogoditi jedinstvena odjava, usluga tipično šalje zahtjev za odjavom prema davatelju identiteta tj. autentikacijskom servisu, a autentikacijski servis onda poduzima daljnje korake kako bi korisnika odjavio sa svih usluga na kojima je trenutno autenticiran. Općenito govoreći, SLO se može obaviti na dva načina:

- odjava u prednjem kanalu (engl. front-channel)
- odjava u pozadinskom kanalu (engl. back-channel)

Odjava u prednjem kanalu se obavlja pomoću web preglednika koji se koristi za slanje HTTP zahtjeva prema određenim URI-ima na uslugama koji služe za odjavu korisnika. Davatelj identiteta će tipično na neki način automatizirati taj postupak, na primjer pomoću skripte u web pregledniku ili učitavanjem URI-a za odjavu pomoću iFrame-a, ili slično. Odjava u pozadinskom kanalu se obavlja tako da autentikacijski servis direktno šalje zahtjeve za odjavom prema uslugama na kojoj je korisnik bio autenticiran (ne koristi se web preglednik).

Postoji mnogo izazova u obavljanju jedinstvene odjave i zna se dogoditi da je implementacija odjave kompliciranija od implementacije autentikacije. Razlog za to je postojanje više sjednica (SSO sjednica i sjednice na samim uslugama) koje je potrebno ukinuti, a ima dosta mjesta gdje stvari mogu poći po krivu. Na primjer, prilikom obavljanja odjave u prednjem kanalu, ako se dogodi greška na strani usluge ili je usluga trenutno nedostupna, daljnji postupak odjave može prestati (web preglednik može ostati "zaglavljen" na usluzi na kojoj se dogodila greška). Također, postoje izazovi u ispravnom konfiguriranju kolačića, jer se zahtjevi za odjavu (kao i za autentikaciju) šalju između različitih domena (davatelj identiteta i davatelj usluge su na različitim domenama), a sve ovisno o tome na koji način se šalju sami zahtjevi (npr. koriste li se HTTP POST zahtjevi ili HTTP GET zahtjevi pomoću redirekcije ili slično). S druge strane, prilikom odjave u pozadinskom kanalu postoje izazovi s uklanjanjem kolačića za vođenje SSO sjednice iz web preglednika.