doi:10.3359/oz1314001

članek

KONCEPT AVTENTIKACIJSKE IN AVTORIZACIJSKE INFRASTRUKTURE V SISTEMU COBISS

Boštjan Batič
Davor Šoštarič

Institut informacijskih znanosti Maribor

Kontaktni naslov:
bostjan.batic@izum.si
davor.sostaric@izum.si

Izvleček

Koncept infrastrukture avtentikacije in avtorizacije predstavlja odmik od ustaljenih načinov "omnia mea mecum porto", kjer vsaka informacijska storitev ali aplikacija (spletna ali namizna) vzdržuje lastni sistem podatkov o uporabnikih. Sistem, zgrajen na podlagi medsebojnega zaupanja, loči avtentikacijski del od avtorizacijskega. Avtentikacija se izvaja v uporabnikovem osnovnem okolju (delovno mesto, izobraževalni proces), avtorizacijski del pa se izvede na podlagi (iz uporabnikovega sveta) pridobljenih in ne interno shranjenih informacij. V sistemu COBISS smo ta koncept že začeli uveljavljati in prikazana sta dva zgleda.

Ključne besede

AAI, avtentikacija, avtorizacija, COBISS, Wi-Fi, brezžično omrežje, Libroam, enotna prijava, SSO, prijavni sistem, ponudnik identitete, IdP, ponudnik storitve, SP, lokalno omrežje

Abstract

The concept of authentication and authorisation infrastructure represents a shift from the standard ways of "omnia mea mecum porto", where every information service or application (both web and desktop) maintains its own system of user data. A system built on mutual trust separates the authentication part from the authorisation part. Authentication is carried out in the user's basic environment (workplace, educational process), while the authorisation part is then carried out on the basis of acquired (from the user's world) and not internally saved information. In the COBISS system, this concept is already being introduced and two examples are shown.

Keywords

AAI, authentication, authorisation, COBISS, Wi-FI, wireless network, Libroam, single sign-on, SSO, login system, identity provider, IdP, service provider, SP, local area network

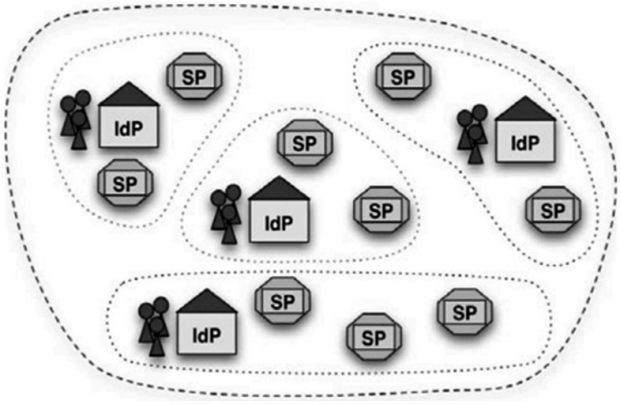
UVOD

Večina zapletenejših storitev na spletu zahteva od uporabnika prijavo, na podlagi katere se ob preverjanju upravičenosti dostopa in uporabe dodelijo še kakšni dodatni atributi, parametri, pravice in podobno. Pri tem vsaka storitev praviloma gradi lastni interni sistem uporabnikovih identifikacij s potrebnimi podatki, kar že pri malo večjem spektru uporabniških želja pripelje uporabnika do precej nelagodnega občutka zaradi obilice uporabniških imen, gesel in podobnih akreditacijskih podatkov. Pri posamičnih izoliranih spletnih storitvah je to še razumljivo. Kadar pa ima uporabnik pravico uporabljati določeno storitev ali aplikacijo na spletu zaradi nespornega dejstva, da mu "to pripada zaradi njegovega statusa v nekem konkretnem okolju", je smiselno, da se del preverjanja pravic prepusti temu okolju. Tipični primer: organizacija, kjer je posameznik zaposlen ali kjer se izobražuje, ima sklenjen formalni dogovor s ponudnikom storitve za možnost uporabe ali dostopa za vse svoje pripadnike z neko skupno lastnostjo (študenti od tretjega letnika dalje, zaposleni na določenem delovnem mestu, gibalno omejeni …). V takem primeru ni stvar ponudnika storitve, da za posameznega uporabnika preverja upravičenost do dostopa, ampak to lahko kvalitetneje, zanesljiveje in predvsem enostavneje ugotovi njegova matična organizacija, ki končno odločitev samo posreduje ponudniku storitve. Eden možnih odgovorov na ta izziv je uporaba infrastrukture za avtentikacijo in avtorizacijo (AAI) in v nadaljevanju se bomo malo pobliže seznanili z osnovno idejo.

PREDSTAVITEV AAI

Infrastruktura za avtentikacijo in avtorizacijo (AAI) omogoča enotno prijavo (angl. *SSO – Single Sign On*) v spletne aplikacije in servise. To pomeni predvsem lažje dostopanje do različnih virov in storitev z enim samim korakom pri prijavi (na primer z uporabniškim imenom in geslom), ki je za uporabnika enoten in neodvisen od prijavnega sistema ponudnika storitve ali aplikacije, ki stoji za njo. Nabor podatkov, ki jih aplikacija sme vedeti o uporabniku, je omejen in pred vsakim vstopom v aplikacijo uporabniku znan. Sama prijava v posamezno spletno aplikacijo ali storitev sestoji iz dveh delov – avtentikacije in avtorizacije.

Za avtentikacijo uporabnika je zadolžen prijavni sistem za avtentikacijo, ki je praviloma urejen v organizaciji (angl. *IdP – identity provider*), kjer je uporabnik zaposlen ali se izobražuje oziroma je v kakršnem koli drugem odnosu z njo. Preverjanje avtorizacijskih podatkov pa opravlja dodatna neodvisna komponenta spletnega strežnika na strani ponudnika aplikacije (angl. *SP – service provider*). Kombinacije IdP-jev in SP-jev so lahko samostojne znotraj posameznih organizacij ali pa se povežejo v večja med seboj priznavajoča se okolja – federacije AAI.

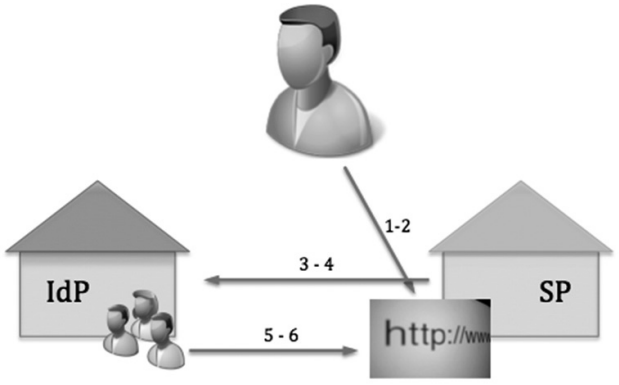


Slika 1: Posamezni IdP-ji in SP-ji v federaciji AAI (objavljeno z dovoljenjem Arnesa)

Tipični potek prijave uporabnika v neko spletno aplikacijo po infrastrukturi AAI poteka po naslednjih korakih (gl. tudi sliko 2):

1. Uporabnik v svoj spletni brskalnik vnese spletni naslov aplikacije.
2. Na prikazani spletni strani ponudnika aplikacije (SP) uporabnik izbere prijavo preko sistema AAI (in običajno ima ponujeno možnost izbire ustrezne federacije AAI, lastne organizacije ali nekega povezovalnega sistema).
3. SP preusmeri uporabnika na prijavni sistem za avtentikacijo (IdP) v domači organizaciji.
4. Uporabnik se pri domačem IdP-ju identificira na način, ki mu je določen (uporabniško ime in geslo, certifikat X.509, posebno geslo za enkratno uporabo …).
5. Po uspešno izvedeni prijavi usmeri IdP uporabnika nazaj na spletno aplikacijo.
6. SP ponovno prestreže zahtevek s sporočilom IdP-ja in uporabniku dovoli dostop do aplikacije.

Ključni avtentikacijski podatki iz četrte točke se ne posredujejo spletni aplikaciji, ampak ostanejo na strani prijavnega sistema – torej pod popolno kontrolo domače organizacije (IdP), ki jih je uporabniku dodelila.



Slika 2: Način povezovanja v spletno aplikacijo preko AAI

Bistveno je, da matične organizacije svojim članom same dodeljujejo dostop do aplikacij tretjih ponudnikov v skladu s svojimi pravili oziroma sklenjenimi dogovori, pogodbami in sporazumi s ponudniki spletnih servisov, zato se le-tem ni treba ukvarjati z dodeljevanjem uporabniških imen, zbiranjem podatkov in preverjanjem statusov o uporabnikih, njihovi upravičenosti do ponujene storitve in podobno. Tipično gre za situacijo, ko neki konkretni SP dodeli pravico do uporabe njegove storitve članom neke organizacije (vsem ali določenemu krogu – npr. študentom, zaposlenim, raziskovalcem …), pri tem pa se ne spušča v to, katera konkretna oseba ima to pravico, saj ta pravica pri posamezniku ni stvar SP-ja, ampak matične organizacije (IdP), ki ji uporabnik "pripada".

Rezultat uporabe koncepta infrastrukture AAI je takó olajšano upravljanje z uporabniškimi identitetami:

- zmanjšanje dela s podatki uporabnikov, saj ni potrebe po dodatnem registriranju in administriranju,
- če organizacija ponuja storitve uporabnikom iz drugih organizacij, ni treba voditi dodatnih evidenc gostujočih uporabnikov,
- uporabniki imajo dostop do številnih domačih in tujih virov, ne da bi jim bilo pri tem treba vzpostavljati, upravljati in vzdrževati različne načine prijavnih sistemov,
- uporabniki niso več vezani na določeno fizično

lokacijo, ampak je dostop določen glede na njihove pravice, kar je v prisojnosti uporabnikove matične organizacije.

Vzpostavljena infrastruktura AAI služi številnim lastnim ter zunanjim aplikacijam in storitvam, kjer se zahteva enostavna, a zanesljiva avtentifikacija in avtorizacija posameznega uporabnika. Zato so zahtevani strožji pogoji, kot smo jih vajeni pri preprostejših okoljih. Predvsem gre za enostavnost in varnost tako s stališča uporabnika kot s stališča upravljavca omrežja. Zahtevana je maksimalna uporabnost na čim več različnih platformah, razširljivost in možnost vpeljevanja novih tehnologij. Administriranja mora biti čim manj.

Pri varnosti gre za dve ravni – uporabnikovo in upravljavčevo. Uporabnik mora dobiti jamstvo, da njegov pretok podatkov ne bo prestrežen oziroma se mu ne prisluškuje (kriptografska zaščita prometa), hkrati se mu ne sme onemogočati uporabe dodatnih varnostnih mehanizmov (na primer IPSec, VPN …). Upravljavcu omrežja morajo biti na voljo mehanizmi za preprečevanje neavtorizirane uporabe ne glede na stopnjo fizičnega varovanja. Zagotovljeno mora biti beleženje dogodkov in s tem omogočeno sledenje morebitnim zlorabam. Uporabljeni morajo biti uveljavljeni standardi, da se ohrani neodvisnost od konkretnih tržnih produktov oziroma proizvajalcev.

Povsem naravno je pričakovati, da bodo uporabniki želeli uporabljati svoje prenosne naprave (prenosne računalnike, dlančnike, tablice, pametne telefone …) doma, na poti, v drugem kraju – skratka povsod po svetu in ne le na svojem delovnem ali učnem mestu v matični organizaciji. Zaradi vpetosti v slovenski in evropski izobraževalno-raziskovalni prostor mora biti rešitev kompatibilna z rešitvami, ki se uveljavljajo v tem prostoru, kajti le tako bodo uporabnikom tovrstne storitve na voljo brez dodatne opreme tudi drugod.

Od prijavnega sistema za avtentikacijo (IdP) se zahteva strežniška postavitev (praviloma na odprtokodni osnovi). V splošnem gre za spletni element, ki overi digitalno identiteto uporabnika, ko le-ta dostopa do spletnih storitev, omogočenih preko infrastrukture AAI. Ne glede na lokacijo spletne storitve se avtentikacija vedno opravi v domači organizaciji uporabnika, kjer se nahaja IdP. S tem dosežemo, da se občutljivi avtentikacijski podatki (na primer geslo) ne posredujejo ponudnikom spletnih storitev.

Na drugi strani se od ponudnika aplikacije ali storitve (SP) pričakuje, da poleg morebitnih lastnih postopkov za prijavo zgradi ustrezen avtorizacijski sistem, ki bo uporabniku najprej omogočil izbiro in uporabo njegovega IdP-ja (torej prijavo v matični organizaciji), v naslednjem koraku pa spoštoval rezultat preverjanja uporabnikovega IdP-ja oziroma sporočilo o uspešnosti prijave. Še več, poleg preprostega odgovora DA/NE o uspešnosti prijave bo ob uporabnikovem soglasju od IdP-ja pridobil še določene dodatne podatke o uporabniku.

Na videz kritični trenutek je uporabnikova prijava, saj mora takrat vpisati svoje uporabniško ime in geslo (ali ekvivalentne zaščitene podatke). V resnici poteka ta postopek preko hierarhičnega sistema strežnikov popolnoma varno. Med uporabnikom in njegovo domačo institucijo se vzpostavi zaščiten tunel in uporabnik se sicer res prijavi v sistem lastne matične organizacije po fizično neznanih kanalih, vendar je pretok podatkov po zaščitenem tunelu varen, saj so povezave kriptirane z najsodobnejšimi šifrirnimi postopki. Osebni podatki v nobenem primeru niso dostopni nikomur izven uporabnikove matične ustanove. Ves postopek preverjanja istovetnosti in upravičenosti do končne uporabe vedno poteka preko posebnih šifrirnih mehanizmov neposredno med uporabnikovo napravo in njegovo matično institucijo. Na ta način ni nevarnosti za prisluškovanje ali prestrezanje prometa med prijavnim postopkom, prav tako ni strahu pred lažnim predstavljanjem; strežnik se namreč predstavi s certifikatom, geslo in uporabniško ime (oziroma elementi za prijavo) pa sta poslana v šifrirani obliki samo strežniku matične organizacije.

Infrastruktura AAI dobi pravo vrednost pri povezovanju več posameznih otočkov SP-jev in IdP-jev na osnovi dogovorjenih enotnih tehnoloških rešitev. Posplošeno lahko federacijo AAI opišemo kot dogovor med člani, da bodo spoštovali ista pravila in tehnološke rešitve, ki bodo omogočile oddaljeno uporabo različnih storitev in virov z zelo poenostavljenim postopkom prijave. Federacija AAI predstavlja okvir zaupanja za vse uporabnike, organizacije in ponudnike ter nastopa kot neodvisno telo, ki skrbi za uveljavljanje dogovorjenih pravil in tehničnih rešitev med člani (ponudniki identitet – IdP) in partnerji (ponudniki storitev – SP).

Potrebe po federacijski infrastrukturi so se v Sloveniji najprej začele pojavljati v izobraževalnem okolju, v knjižnicah in raziskovalnih ustanovah. Prve analize pokazale, da si uporabniki želijo:

- dostop do spletnih učnih okolij,
- vzpostavitev učnih okolij na tehnologiji Moodle,
- dostop do videokonferenčne tehnologije,
- dostop do varovanih vsebin na posameznih fakultetah,
- dostop do konzorcijskih tujih virov literature (Elsevier, Science Direct in Ebscohost).

PRAKTIČNI PRIKAZ

V tem razdelku bomo prikazali dva praktična načina uporabe avtentikacijske in avtorizacijske infrastrukture v knjižnicah, ki so vključene v sistem COBISS.SI. Prvi način dokaj enostavno omogoča dostop do interneta v knjižnicah za uporabnike z lastnimi napravami (prenosniki, tablicami, pametnimi telefoni ipd.), drugi način pa rešuje problematiko upravljanja uporabnikovih pravic pri dostopu do svetovnih ponudnikov baz podatkov in informacijskih servisov (predvsem v večjih knjižnicah, na primer univerzitetnih).

Libroam

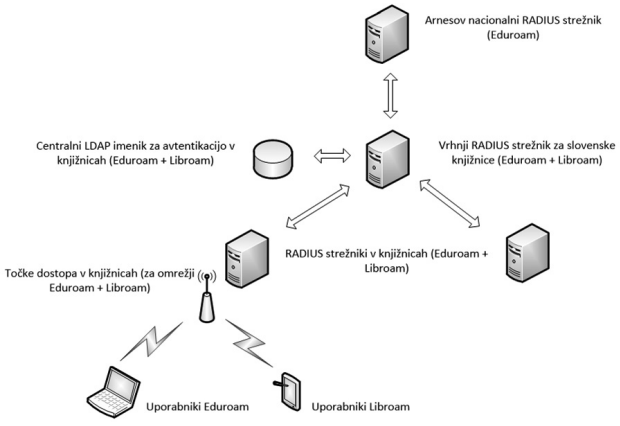
S prihodom brezžičnih lokalnih omrežij so se možnosti dostopa do interneta v knjižnicah močno povečale, saj knjižnice ne potrebujejo več velikih vlaganj v komunikacijsko opremo za te namene.

Sama tehnologija brezžičnih omrežij je znana – na eni strani imamo točko dostopa (angl. *access point*), povezano v lokalno omrežje in internet, na drugi pa uporabnikovo napravo, vmes so radijski valovi, vse skupaj pa opisuje standard IEEE 802.11.

Vendar tehnologija ni vse in ni vseeno, kako bo knjižnica zastavila svojo politiko dostopa v svetovna omrežja. Vsekakor ima vse možnosti, da si na svojem lokalnem omrežju vzpostavi ustrezne točke dostopa in določi lastni režim uporabe za svoje zaposlene kot tudi redne ali občasne obiskovalce. Osnovna dilema za upravitelja lokalnega omrežja v knjižnici je odločitev med popolnoma odprtim dostopom na eni strani in kontroliranim dostopom na drugi. V prvem primeru prevzema knjižnica vso odgovornost za morebitna nekorektna ravnanja svojih članov (vključno z varnostno problematiko lastnega omrežja). Če pa ne dovoli odprtega dostopa, si nakoplje ogromno administrativnega dela – odgovoriti si je treba vsaj na vprašanja o postopkih dodeljevanja gesel, možnosti generičnih začasnih gesel, individualizaciji trenutnih gesel, poskrbeti za evidentiranje in arhiviranje metapodatkov o prometu, urediti upravljanje z uporabniškimi računi in še in še. Ne nazadnje so možne še vmesne poti, na primer dogovor s komercialnim ponudnikom brezžičnega dostopa ali z altruističnim skrbnikom, ki omogoča odprt prost dostop (na primer krajevna oblast, časopisna hiša, veleposlaništvo tuje države ali pa neprevidni lastnik domače stanovanjske postavitve – vse to smo v našem okolju že srečali).

Knjižnice, vključene v sistem COBISS.SI, imajo možnost uporabe brezžičnega omrežja Libroam, za katerega skrbi Institut informacijskih znanosti Maribor (IZUM) in ga kot standardno storitev ponuja knjižnicam in njenim članom oziroma uporabnikom. Z uporabo tega omrežja člani knjižnice varno dostopajo do interneta s svojimi lastnimi napravami. Libroam dopolnjuje že obstoječo storitev Moja knjižnica. Ključnega pomena je dejstvo, da so relevantni podatki uporabnikov storitve Moja knjižnica že znani in verodostojni. Tako odpade potreba po dodatnem zbiranju podatkov o uporabnikih, administraciji uporabniških računov in podobno.

Ko uporabnikova naprava zazna brezžično omrežje Libroam, pošlje preko točke dostopa zahtevo za povezavo. Knjižnica ima za ta namen posebni strežnik, ki zahtevo za povezavo posreduje vrhnjemu strežniku na IZUM-u, kjer se vsi uporabniki Libroam identificirajo. Ko mobilna naprava preveri strežnikov certifikat, se med njima ustvari zaščiten komunikacijski tunel in tako se po varni šifrirani povezavi izvede avtentikacija. Če je uspešna, se informacija vrne strežniku v knjižnici, ki uporabniku omogoči povezavo v brezžično omrežje in svet.



Slika 3: Prikaz povezovanja v omrežje Libroam

Libroam je primer varnega brezžičnega omrežja. Ves promet med točko dostopa in odjemalcem je šifriran, istovetnost strežnika in uporabnika pa potrjena. Varnostni mehanizmi omrežja Libroam zagotavljajo vsaj takšno stopnjo varnosti, kot jo zagotavlja ožičeno omrežje.

Dostop do svetovnih ponudnikov informacijskih storitev

V knjižničnem sistemu COBISS imajo posamezni polnopravni člani svoje ločene poslovne odnose z nekaterimi svetovnimi ponudniki storitev. Še do nedavnega je prijava v te sisteme temeljila bodisi na posebnih uporabniških geslih ali pa so bile storitve omogočene samo za dogovorjene IP-naslove. Vse več velikih svetovnih ponudnikov danes omogoča avtentikacijo in avtorizacijo tudi preko infrastrukture AAI. Z drugimi besedami – priznavajo pristojnost uporabnikove matične organizacije, da sama preveri in

določi stopnjo upravičenosti dostopa svojih uporabnikov ter obseg njihovih pravic. Eden takih izjemno popularnih informacijskih portalov je Web of Science (WoS), ki omogoča dostop do multidisciplinarnih bibliografskih baz podatkov z indeksi citiranosti Science Citation Index Expanded® (SCI-EXPANDED), Social Sciences Citation Index® (SSCI) in Arts & Humanities Citation Index® (A&HCI). Uporabniki knjižnic, članic sistema COBISS.SI, ki imajo za uporabo WoS sklenjene ustrezne sporazume, lahko vzpostavijo dostop do teh servisov, aplikacij in podatkov tudi s pomočjo infrastrukture AAI. Tako na primer študentu iz slovenske univerze ni treba skrbeti za uporabniško ime ali račun, geslo in podobne akreditacije, prav tako pri svojem delu ni omejen izključno na svojo fizično prisotnost v lokalnem univerzitetnem omrežju. Pri svojem dostopu bo ob obisku spletne strani WoS preusmerjen v okolje svoje matične organizacije, kjer se bo prijavil na svoj običajni način (uporabniški račun, geslo, certifikat …). Postopek ugotavljanja pravilnosti prijave izvaja njegova domača organizacija, ki vzpostavi varen in šifriran tunel z WoS, ki ne dobi od matične organizacije nikakršnih občutljivih podatkov o uporabniku (na primer geslo …), ampak le potrditev, da ima uporabnik vse dogovorjene pravice za uporabo storitev WoS.

Slika 4: Prijava na Web of Science in izbira ustrezne AAI

Kot je razvidno iz slike 4, se je uporabnik na spletni strani WoS odločil za vstop preko infrastrukture AAI. Na voljo je dobil seznam različnih infrastruktur AAI, med katerimi bo izbral svojo. Potem se bo prijavil v svoje domače okolje, WoS pa bo to *avtentikacijo* priznal. V fazi *avtorizacije* mu bo potem WoS dovolil uporabo svojih določenih storitev, določenih pa morda tudi ne, glede na morebitna dodatna določila, ki jih ima uporabnik zapisana pri svoji matični organizaciji.

Uporabniki v Sloveniji, ki omenjeno storitev WoS uporabljajo na podlagi sklenjenih konzorcijskih dogovorov mimo infrastrukture AAI, so pri svoji uporabi praviloma vezani na fizično prisotnost na določenem lokalnem omrežju ustanove, ki je članica konzorcija, saj jih ponudnik storitve WoS sam avtenticira in avtorizira preko vnaprej dogovorjenega obsega naslovov IP. Uporabnik iz prejšnjega odstavka teh omejitev nima, saj se sam ponudniku storitve WoS neposredno ne predstavlja; WoS kot ponudnik storitve popolnoma verjame in zaupa odločitvi uporabnikove matične organizacije.

NOVE MOŽNOSTI

Knjižnice v sistemu COBISS imajo v svojih podatkovnih bazah vse bistvene podatke o svojih uporabnikih, tako da so dani vsi pogoji, da prevzamejo vlogo IdP. Tisti uporabniki, ki uporabljajo storitev Moja knjižnica, imajo že dodeljena ustrezna uporabniška imena in gesla, tako da ni potrebe po nikakršnem podvajanju akreditacijskih sistemov za posamezne nove namene. Potrebna je le dosledna politika knjižnice pri izboru tehnologije in informacijskega okolja, načina upravljanja virov in pogajanja s ponudniki in podobno, na drugi strani pa zavest, da so vsi relevantni podatki že zbrani. Nadaljnje možnosti so praktično neomejene: odpiranje vstopa v posamezne prostore (na primer čitalnice), uporaba dodatnih naprav (na primer fotokopirni stroji, tiskalniki …), avtomati za prigrizke in napitke, dvig parkirnih zapornic … skratka vse, kjer je na neki način treba preveriti uporabnika in se na podlagi zbranih podatkov o njem odločiti, ali in v kolikšni meri je upravičen do konkretne storitve. Z dobro premišljenim sistemom AAI v lokalnem okolju odpadejo vsa ponavljajoča se dejanja v zvezi s "prepoznavanjem" uporabnika in "priznavanjem" njegovih karakteristik. Še več – z enotnim konceptom infrastrukture AAI v vseh knjižnicah, vključenih v nacionalne sisteme COBISS in v regionalno mrežo COBISS.Net, so ustvarjeni vsi pogoji za medsebojno priznavanje uporabnikovih identitet in lahko bomo govorili o še eni novi federaciji AAI.

ZAKLJUČEK

Na podlagi zapisanega o konceptu avtentikacijske in avtorizacijske infraskture lahko povzamemo:

- odnosi so vzpostavljeni v trikotniku uporabnik – matična organizacija s svojim prijavnim sistemom za avtentikacijo (IdP) – ponudnik storitve (SP),
- uporabnik ne potrebuje kopice uporabniških imen, gesel itd. za vsako storitev, do katere je upravičen kot pripadnik neke matične ustanove (organizacija, šola, knjižnica …),
- preverjanje identitete, upravičenosti, statusa, pravic in podobno je porazdeljeno med IdP in SP ter izločeno iz neposrednega odnosa med SP in uporabnikom,
- avtentikacijo za uporabo storitev, ki jih ponujajo zunanji dobavitelji, izvaja za svoje uporabnike matična organizacija (IdP),
- uporabnik se ne prijavlja v prijavni sistem ponudnika storitve (SP), ampak v prijavni sistem matične organizacije (IdP),
- pretok podatkov v fazi prijave je kriptiran in poteka po varnem zaščitenem tunelu,
- avtorizacijo posameznih pravic izvede SP na podlagi podatkov, ki jih dobi od IdP.

Čeprav je bilo na začetku skoraj povsod potrebno obilo prepričevanja in tudi razbijanja konformističnih tabujev, so izkušnje z vzpostavitvijo infrastrukture AAI izjemno pozitivne, statistike uporabe impresivne, uporabniški odzivi pa nas dodatno prepričujejo v upravičenost uveljavljanja tega koncepta. V knjižnicah, vključenih v sistem COBISS.SI, uporaba strmo narašča. Knjižnice so spoznale, da jim je ogromno dela z upravljanjem pravic uporabnikov prihranjenega, uporabniki (posebno v večjih okoljih) pa so navdušeni nad možnostmi novih obzorij. Koncept infrastrukture AAI, ki ga uporabljamo, je vsaj kompatibilen, če že ne identičen tistemu, ki ga uporabljajo največja svetovna akademska in raziskovalna okolja. Počasi se zmanjšuje nezaupanje med posameznimi IdP-ji, pomemben preboj pa je tudi uspešno povezovanje v slovensko nacionalno izobraževalno in raziskovalno federacijo AAI, ki jo upravlja Arnes, ki so jo priznali nekateri največji svetovni ponudniki storitev. Pridobljene izkušnje in znanje so na voljo vsem, ki imajo interes vzpostaviti podobna okolja.

Reference

[1] TERENA (2011). What is Eduroam. Dostopno na: http://www.eduroam.org.

[2] Arnes (2013). Federacija izobraževalnih omrežij Eduroam. Dostopno na: http://www.eduroam.si.

[3] Šoštarič D. (2009). Eduroam – brezžično omrežje v izobraževalnih in raziskovalnih okoljih. V: Povežimo informacijske otoke: Zbornik konference Informatika v javni upravi. Brdo pri Kranju.

[4] Javni razpis št. 430-76/2008 – Razpisna dokumentacija. MŠZT, 2011.

Spletne povezave

- http://aai.arnes.si
- http://www.internet2.edu/shibboleth
- http://www.switch.ch/aai/demo/
- http://home.izum.si/cobiss/libroam/