doi:10.3359/oz1401003

članek

FEDERACIJA COBISS AAI

AVTENTIKACIJSKO-AVTORIZACIJSKA INFRASTRUKTURA COBISS

Miran Petek
Boštjan Batič
Stašo Vobič
Vojko Ambrožič
Matjaž Cigrovski
Miro Kolarič

Institut informacijskih znanosti Maribor

Kontaktni naslovi:
miran.petek@izum.si
bostjan.batic@izum.si
staso.vobic@izum.si
vojko.ambrozic@izum.si
matjaz.cigrovski@izum.si
miro.kolaric@izum.si

Izvleček
IZUM in knjižnice ponujajo svojim uporabnikom številne informacijske servise in večina od teh zahteva prijavo uporabnika. Prijava se izvaja na osnovi uporabniškega imena in gesla ter omogoča avtentikacijo in avtorizacijo uporabnika. IZUM tovrstni mehanizem upravlja na osnovi identitetnih in drugih podatkov o članih v sistemu COBISS. V letošnjem letu smo vpeljali enotno prijavo (angl. *single sign-on*) preko programske komponente Shibboleth in Federacije COBISS AAI.

Ključne besede
informacijski sistemi in servisi, COBISS.SI, COBISS/Izposoja, avtentikacija, avtorizacija, AAI, Federacija COBISS AAI, Federacija ArnesAAI, Shibboleth, LDAP, SimpleSAMLphp, IdP, Identity Provider, SP, Service Provider

Abstract
IZUM and libraries offer their users numerous information services and most of them require user login. Login is carried out on the basis of a username and password and enables the user's authentication and authorisation. IZUM manages such a mechanism based on identity data and other information about the members within the COBISS system. This year, a single sign-on system was introduced via the Shibboleth software component and the COBISS AAI Federation.

Keywords
information systems and services, COBISS.SI, COBISS/Loan, authentication, authorisation, AAI, COBISS AAI Federation, ArnesAAI Federation, Shibboleth, LDAP, SimpleSAMLphp, IdP, Identity Provider, SP, Service Provider

UVOD

Knjižnice ponujajo svojim uporabnikom številne spletne informacijske servise in večina od teh zahteva prijavo uporabnika. To velja še posebej za tiste informacijske servise, ki omogočajo personalizacijo storitev, tj. nastavitve, ki si jih lahko uporabniki nastavijo po svoji presoji, s čimer servis prilagodijo svojim željam in potrebam. Pri tem se zastavlja vprašanje, kakšen prijavni mehanizem uporabiti. Najprej je treba ugotoviti, ali se od uporabnika zahteva le avtentikacija ali tudi avtorizacija, kar je odvisno od storitve, ki jo knjižnica ponuja svojim uporabnikom, in od licenčnih dogovorov, ki jih imajo knjižnice s ponudniki informacijskih servisov.

Obstajajo številni avtentikacijsko-avtorizacijski sistemi. LDAP (angl. *Lightweight Directory Access Protocol*) se največkrat uporablja v knjižničnih informacijskih sistemih. Zagotavlja zadostno mero splošne informacijske varnosti in tudi varnosti osebnih podatkov. Na Institutu informacijskih znanosti (IZUM) podpiramo avtentikacijske rešitve LDAP in jih ponujamo slovenskim knjižnicam. Rezultat so številni že realizirani projekti, kar bo med drugim predstavljeno v nadaljevanju prispevka.

Nadgradnjo protokola LDAP predstavlja dopolnitev s programskim modulom Shibboleth, ki omogoča enotno prijavo uporabnika v različne informacijske servise, s čimer odpravlja potrebo po ponovnih prijavah uporabnika. Federacija COBISS AAI je rezultat projekta enotne prijave na osnovi podatkov o članih knjižnic v sistemu COBISS; zagotavlja avtentikacijsko in avtorizacijsko infrastrukturo za prijavo uporabnikov v informacijske servise, ki jih knjižnice ponujajo svojim uporabnikom.

Članek je nastal na osnovi prispevka avtorjev Mirana Petka in Pera Šobota z naslovom *Autenikacijsko-autorizacijska rješenja COBISS i šiboletizacija internet servisa*, ki je bil predstavljen na 11. mednarodni konferenci Juni na Uni v Bihaću (2014).

INFORMACIJSKI SERVISI V SLOVENSKIH KNJIŽNICAH

Slovenske knjižnice uporabljajo številne informacijske spletne servise. V nadaljevanju bomo predstavili nekatere od teh.

Brezžični dostop do spleta

Brezžični dostop do spleta se v današnjem času mobilnih naprav razume kot storitev, brez katere knjižnica ne more zadovoljiti želja sodobnega uporabnika. V akademskem in raziskovalnem okolju se je uveljavil brezžični dostop do spleta preko mednarodnega projekta Eduroam (https://www.eduroam.org/), za katerega v Sloveniji skrbi Arnes (http://www.arnes.si/). Gre za globalni servis brezžičnega dostopa iz prostorov izobraževalnih institucij, ki so članice projekta. To so univerze, raziskovalni inštituti, srednje in osnovne šole ter tudi vrtci, ki zaposlenim, študentom ter raziskovalcem omogočajo varno in enostavno uporabo njihovih mobilnih naprav (notesnik, tablica, pametni telefon) pri dostopu do spleta. Dodana vrednost tega servisa je možnost uporabe servisa na vseh lokacijah institucij po svetu, ki sodelujejo v projektu Eduroam. Trenutno sodeluje 54 držav. V praksi to pomeni, da je npr. servis dostopen slovenskemu profesorju ali študentu med obiskom ali študijem na tuji univerzi zunaj Slovenije.

Za preostale knjižnice IZUM na osnovi enake infrastrukture, kot je Eduroam, ponuja brezžični dostop do spleta preko servisa Libroam (http://home.izum.si/cobiss/libroam/). Servis uporabljajo predvsem splošne knjižnice, katerih uporabniki niso upravičeni do uporabe storitev Arnesa. Libroam uporabljata tudi Narodna in univerzitetna knjižnica v Ljubljani ter Univerzitetna knjižnica Maribor, ki to storitev ponujata ne le univerzitetnim uporabnikom, pač pa tudi drugim članom knjižnice. To omrežje lahko uporabljajo tudi uporabniki omrežja Eduroam, saj se uporablja enaka tehnološka platforma, kar zagotavlja kompatibilnost obeh omrežij.

Oddaljeni dostopi do informacijskih servisov

EZproxy (http://www.oclc.org/ezproxy.en.html) je v svetu najpogosteje uporabljeno orodje za zagotavljanje storitev oddaljenega dostopa do informacijskih virov. Ponudnik programske opreme je OCLC (http://www.oclc.org/). Tudi v Sloveniji je to orodje zelo razširjeno, saj omogoča oddaljen dostop do servisov ne glede na fizično lokacijo uporabnika (tudi od doma). Primarni način dostopa do informacijskih virov se ureja na osnovi IP-naslovov institucij; ker pa ponudniki informacijskih virov ne dovoljujejo registracije IP-naslovov zunaj institucij, ki so naročnice servisov, je prav orodje EZproxy zelo priročen servis za zagotavljanje oddaljenega dostopa. S postopkom avtorizacije, ki jo omogoča tehnologija LDAP, pa je zagotovljeno, da storitev uporabljajo samo tisti, ki so do nje upravičeni.

Orodje EZproxy uporablja Univerza v Ljubljani preko portala Mrežnik (http://www.nuk.uni-lj.si/nuk/mreznik.asp), za katerega skrbi Narodna in univerzitetna knjižnica. Tudi Univerza v Mariboru uporablja to orodje, in sicer preko portala Univerzitetne knjižnice Maribor (http://www.ukm.si/podrocje.aspx?id=1126). Splošne knjižnice imajo prav tako naročene številne informacijske vire in urejajo oddaljeno prijavo z orodjem EZproxy. V IZUM-u zagotavljamo to možnost dostopa do informacijskih virov za preostale knjižnice, ki nimajo svojih rešitev za oddaljeni dostop preko portala http://home.izum.si/izum/ft_baze/oddaljen_dostop.asp.

Baze podatkov in metaiskalniki

Med najpomembnejše storitve knjižnic vsekakor sodijo dostopi do baz podatkov. V Sloveniji je ponudba zelo široka. Obstajajo nacionalni konzorciji za nabavo baz podatkov in e-virov, ki vključujejo vse univerzitetne uporabnike in najpomembnejše raziskovalne institucije. Veliko je tudi individualnih dogovorov med ponudniki informacijskih virov in posameznimi knjižnicami. Založniki, agregatorji in drugi ponudniki specializiranih baz podatkov ponujajo slovenskim knjižnicam pester nabor vsebine, tako z akademsko tematiko kot tudi tematiko, zanimivo za splošne uporabnike. Še posebej so zanimive baze podatkov s celotnimi besedili in v zadnjem času tudi e-knjige. Knjižnice se vse pogosteje odločajo za tovrstna naročila, ki nadomeščajo klasične tiskane izdaje. Nekatere knjižnice prehajajo na modele naročnin, ki zajemajo samo elektronske vire (angl. *e-only*).

Metaiskalniki in druga napredna iskalna orodja (angl. *discovery tools*) uporabnikom olajšajo iskanje informacij in literature, ki jo potrebujejo za svoje raziskovalno-izobraževalne potrebe. V IZUM-u ponujamo storitev Metaiskalnik (http://home.izum.si/izum/metaiskalnik/), ki omogoča hkratno iskanje po različnih informacijskih virih. S tem orodjem je uporabniku prihranjen čas, potreben za izbiro posameznih informacijskih virov in za izvajanje poizvedb na različnih portalih in grafičnih vmesnikih z različnimi iskalnimi tehnikami. Napredna iskalna orodja (angl. *discovery tools*), ki so v svetu v porastu in počasi izpodrivajo klasične knjižnične portale za iskanje informacij, to delo uporabnikom lajšajo, saj je iskanje po centralnem indeksu precej hitrejše, enostavnejše in uporabniku prijaznejše. Tudi v Sloveniji so ta orodja že v uporabi in IZUM v svojem programu dela načrtuje implementacijo rešitve v okviru sistema COBISS/OPAC.

Moja knjižnica v COBISS/OPAC-u

Moja knjižnica je ena izmed najpomembnejših funkcionalnosti COBISS/OPAC-a (http://www.cobiss.si). Omogoča vpogled v izposojeno gradivo posameznega člana in možnost online podaljševanja. Online rezervacije gradiva so prav tako zelo uporabna storitev, ki skupaj z medknjižnično izposojo uporabniku omogoča naročanje gradiva iz "domačega naslanjača". Mobilna aplikacija mCOBISS (http://m.cobiss.si/) še dodatno pripomore k lagodnosti uporabe servisa. Ena od funkcij, ki so jo uporabniki želeli in je bila v zadnjem času dodana v Mojo knjižnico, je pregled zgodovine izposojenega gradiva. Seveda pa ne smemo pozabiti na pregled nad dolgovi in omejitvami, ki jih imajo uporabniki v svoji knjižnici. Možnost vklopa obveščanja po e-pošti ali preko SMS-a lahko uporabnikom olajša nadzor nad pravočasnim vračanjem gradiva in prejemanjem različnih obvestil knjižnice o dogodkih in pomembnejših informacijah. Vsekakor pa se funkcionalnosti Moje knjižnice širijo z vsako novo verzijo COBISS/OPAC-a.

Spletni forumi, spletni tečaji …

Zelo uporabne strokovne diskusije o knjižničarskih temah se pogosto razvijajo na spletnih forumih. Tudi IZUM na spletnem naslovu http://home.izum.si/cobiss/e-forumi/ ponuja tri takšne e-forume. Udeleženci razpravljajo o katalogizaciji, splošnem geslovniku COBISS in referenčnem servisu Vprašaj knjižničarja ter s tem pripomorejo k boljšemu razumevanju tematike in tudi pomagajo pri oblikovanju vizije nadaljnjega razvoja posameznih področij. Spletno učenje (http://izobrazevanje.izum.si/), ki ga v IZUM-u ponujamo na osnovi orodja Moodle, je zelo uporaben pripomoček za učenje in usposabljanje naših uporabnikov, in sicer še posebej končnih uporabnikov knjižnic, ki jim na osnovi video vsebin, pripravljenih nalog, testov ter možnosti samostojnega učenja pomagamo pridobivati znanje o iskanju informacij v sistemu COBISS/OPAC in drugih informacijskih virih, kot so Web of Science, ProQuest in EBSCO.

Drugi servisi, ki jih ponujajo knjižnice

Med zanimivejše knjižnične servise sodi storitev "Odpiranje vrat", ki jo uporabljata Univerzitetna knjižnica Maribor ter Narodna in univerzitetna knjižnica, Ljubljana. Člani njunih knjižnic lahko s člansko izkaznico odpirajo vrata v določene knjižnične prostore, kot je npr. čitalnica. V Ljubljani je zaživel projekt Urbana (http://www.jhl.si/enotna-mestna-kartica-urbana), ki omogoča uporabo knjižničnih storitev s pametno kartico; ista pametna kartica omogoča tudi uporabo drugih storitev Mestne občine Ljubljana, npr. uporabo javnega mestnega avtobusnega prevoza, parkiranje, obiskovanje muzejev. Številne knjižnice uporabljajo knjigomate, ki olajšajo vračanje izposojenega knjižničnega gradiva. Pojavljajo se tudi novi servisi upravljanja s tiskanjem vsebin na tiskalnik (npr. PaperCut), kar predstavlja dodatno ponudbo knjižnic. Večina knjižnic uporabnikom zagotavlja dostop do osebnih računalnikov na lokacijah knjižnice. Portali elektronskih knjig, kot je npr. Biblos (http://www.biblos.si/lib/), prvi slovenski portal tovrstne ponudbe, omogočajo izposojo ali nakup e-knjig. Tovrstnih servisov je iz dneva v dan več in pričakovati je, da bo ponudba knjižnic tudi v prihodnje raznolika in prilagojena sodobnemu načinu življenja.

Ni namen tega prispevka podrobneje opisati ponudbo knjižnic, ki je prisotna v slovenskem knjižničnem prostoru. Precej je o tem pisal že Pero Šobot (2013). Vsem omenjenim servisom je skupno dejstvo, da zahtevajo prijavo uporabnika, tj. vnos uporabniškega imena in gesla, s katerim uporabnik dokaže svojo identiteto v svoji knjižnici in s tem upravičenost do dostopa. V omenjene servise se je treba prijaviti zaradi avtorizacije, ki jo informacijski servis od uporabnika zahteva, ali zaradi personalizacije nastavitev, ki jih uporabnik v servisu uporablja (npr. shranjevanje uporabljenih iskalnih zahtev, nastavitve uporabniškega vmesnika, vklop storitev obveščanja itd.), ali zaradi obojega. Pogoj za možnost prijave je obstoj elektronske baze podatkov o članih knjižnice.

BAZE PODATKOV O ČLANIH KNJIŽNICE V SISTEMU COBISS

Večina slovenskih knjižnic uporablja avtomatizirano izposojo gradiva, ki jo omogoča segment COBISS/Izposoja in predstavlja eno od pomembnejših lokalnih aplikacij knjižničnega informacijskega sistema COBISS. Pomemben del tega segmenta je baza podatkov o članih knjižnice (evidenca članov). Knjižničarji imajo možnost vpisovanja, ažuriranja in brisanja osebnih podatkov o članih v svoji lokalni bazi. Segment izposoje omogoča poleg izposoje gradiva tudi podaljševanje roka izposoje, vračanje, rezervacije in evidentiranje izgubljenih izvodov gradiva, evidentiranje in poravnavo terjatev do članov ter iskanje in izpis podatkov o članu, izdelavo in brisanje opominov, vpis opomb o članih in številne druge funkcije. Skratka, evidenca članov knjižničarjem omogoča vpogled v podatke in aktivnosti posameznih članov knjižnice.

Večina vpisovanja in ažuriranja podatkov o članih se izvaja ročno, možen pa je tudi samodejni vnos. V Sloveniji se podatki samodejno ažurirajo predvsem v univerzitetnih knjižnicah, kjer obstajajo univerzitetne evidence študentov, zapisane v referenčni bazi podatkov, ki jo v sodelovanju z računalniškima centroma Univerze v Ljubljani in Univerze v Mariboru v IZUM-u pripravimo za vsako študijsko leto. Za tiste študente, ki so že vpisani v lokalno

bazo podatkov o članih knjižnice, se podatki povežejo z aktualnimi podatki iz referenčne baze podatkov, ki pa služi tudi za poenostavljen vpis novega člana – študenta, saj se ob vpisu v knjižnico večina podatkov prenese iz referenčne baze. Pripravljamo tudi rešitve, ki bodo omogočale neposreden zajem in ažuriranje podatkov iz že pripravljenih evidenc in registrov Ministrstva za izobraževanje, šolstvo in šport Republike Slovenije.

Omenimo naj le nekaj podatkov, ki se lahko beležijo pri posameznem članu knjižnice in so pomembni za prijavo uporabnika v informacijske servise. Vpisna številka člana zagotavlja enolično identifikacijo člana v posamezni knjižnici in se uporablja pri avtentikaciji, tj. dokazovanju identitete v knjižnici. Kategorija člana (študenti, zaposleni, upokojenci, zaposleni na univerzi, zaposleni v matični ustanovi itd.) predstavlja tudi enega pomembnejših podatkov o članu, ki se velikokrat uporabi za avtorizacijo člana ali kot kriterij za določanje pristojnosti članu (npr. omogočen dostop do licenčnih informacijskih virov). Evidentirajo se lahko tudi številni drugi podatki za identifikacijo članov (ime in priimek, številka indeksa, številka osebnega dokumenta), osebni podatki (datum rojstva, spol, kraj rojstva itd.), podatki o izobrazbi in družinskih članih, starših in skrbnikih ter številni drugi podatki.

Za identifikacijo člana se poleg vpisne številke člana lahko uporabi tudi kakšna druga (enolična) identifikacijska številka, kot npr. številka indeksa, 17-mestna uid-številka RFID-kartice itd. Pogoj je le, da je v lokalni bazi podatkov o članih ta podatek vpisan na ustreznem mestu.

V IZUM-u posvečamo posebno pozornost dostopu do občutljivih osebnih podatkov. V Sloveniji velja zelo strog Zakon o varstvu osebnih podatkov (ZVOP-1), ki na področju zagotavljanja zasebnosti in varnosti osebnih podatkov nalaga obveznosti in odgovornosti tako ponudniku informacijskih servisov (npr. IZUM) kot tudi knjižničarjem, ki delajo v segmentu avtomatizirane izposoje gradiva.

AVTENTIKACIJSKO-AVTORIZACIJSKI PROTOKOLI

V prvem delu prispevka so bili predstavljeni nekateri informacijski servisi, ki jih knjižnice ponujajo svojim uporabnikom. Ugotavljamo lahko, da bo ponudba tovrstnih spletnih storitev v prihodnje vse večja in vse bolj prilagojena potrebam uporabnikov. To vključuje tako mobilnost in interaktivnost kot tudi družabna omrežja, ki jih prinašajo sodobna tehnologija in način izobraževanja ter življenjski slog uporabnikov na splošno.

Številne spletne storitve omogočajo uporabniku prijazne funkcionalnosti, ki uporabniku olajšajo delo in prilagodijo orodje osebnostnim preferencam posameznika. Podpirajo personalizacijo nastavitev. Uporabnik si lahko znotraj spletnega vmesnika posamezne aplikacije shrani že uporabljene iskalne zahteve, s čimer prihrani čas, saj mu ni treba ponovno vpisovati iskalnega izraza, ki ga je uporabil že kdaj prej. Ponudniki v svojih orodjih ponujajo tudi možnost obveščanja o posameznih dogodkih po e-pošti, kot npr. obveščanje o objavi novega članka posameznega avtorja ali nove številke revije. Nekateri servisi dopuščajo možnost prilagoditve vmesnika aplikacije (barve, logotipi …), kar uporabniku spletno mesto približa zaradi njemu prijaznejšega spletnega okolja. Nekateri iskalniki omogočajo z osebnostnimi nastavitvami vpliv na algoritem relevance, ki ga iskalnik uporablja – uporabnik npr. določi stopnjo svoje izobrazbe ali izbere želeno raziskovalno področje. Skratka, dodatna ponudba funkcionalnosti je zelo pestra. Vendar pa se mora uporabnik prijaviti ali avtenticirati, če želi to ponudbo uporabljati. Če se uporabnik ne prijavi, teh dodatnih funkcionalnosti ne more uporabljati, uporablja lahko le privzete osnovne funkcije. Nekateri informacijski servisi pa zaradi licenčnih pogojev zahtevajo prijavo uporabnika že zgolj za osnovno uporabo servisa. Primeri takšnih informacijskih servisov so Web of Science, ProQuest, Scopus, EBSCOhost itd.

Za prijavo uporabnika v spletne servise potrebujemo podatke o članih. Ugotovili smo že, da imajo slovenske knjižnice baze podatkov o svojih članih v segmentu COBISS/Izposoja. Druga zahteva za dostop do servisov pa je avtentikacijsko-avtorizacijski protokol, ki bo zagotovil povezljivost med bazami podatkov o članih knjižnic in informacijskimi servisi teh knjižnic.

Obstajajo številni protokoli, ki zagotavljajo to povezljivost: LDAP, SIP, CAS, RADIUS, Shibboleth, CGI in drugi. V IZUM-u smo sprva uporabljali protokol SIP2, ki pa smo ga v zadnjem obdobju nadomestili s protokolom LDAP in ga v letošnjem letu nadgradili s programskim modulom Shibboleth. V nadaljevanju bodo predstavljene tovrstne rešitve.

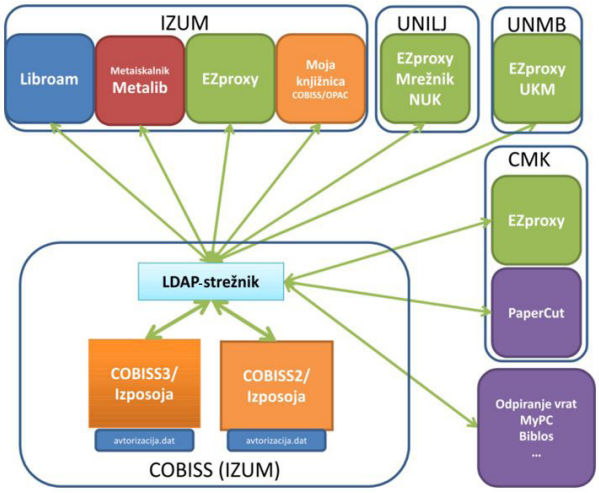
PROTOKOL LDAP

LDAP (angl. *Lightweight Directory Access Protocol*) je najpogosteje uporabljen avtentikacijski protokol v knjižničnih informacijskih servisih. S protokolom SSL (angl. *Secure Sockets Layer*) zagotavlja preko privzetih vrat 636 zadovoljiv nivo tako splošne varnosti informacijskih sistemov kakor tudi varnosti osebnih podatkov, ki jih določa Zakon o varstvu osebnih podatkov (ZVOP-1).

V osnovi je za avtentikacijo uporabnikov potreben imenik uporabnikov LDAP; ker pa knjižnice že uporabljajo svoje baze podatkov o članih v COBISS-u, smo v IZUM-u vzpostavili strežnik LDAP za komunikacijo med bazami podatkov o članih in informacijskimi servisi po standardnem protokolu LDAP. Imenik uporabnikov LDAP ponujamo le nekaterim slovenskim institucijam, ki nimajo možnosti avtomatizirane izposoje gradiva (in s tem baze podatkov o članih) ali celo nimajo svoje knjižnice. Takšen primer je Agencija za raziskovalno dejavnost RS, za katero IZUM zagotavlja gostovanje LDAP.

Slika 1: Osnovni koncept prijavnega mehanizma COBISS preko protokola LDAP

Slika 1 prikazuje osnovni koncept prijavnega mehanizma COBISS preko protokola LDAP. Dostop do informacijskega servisa (npr. Libroam, Moja knjižnica v COBISS/OPAC-u, EZproxy, Metaiskalnik, Mrežnik itd.) zagotavlja strežnik LDAP na osnovi podatkov o članih iz COBISS/Izposoje preko protokola LDAP. Uporabnik ob prijavi v informacijski servis vpiše uporabniško ime in geslo, ki se preverita v bazi podatkov o članih. Če sta uporabniško ime in geslo pravilna, bo uporabniku prijava v informacijski servis omogočena, sicer pa bo prijava zavrnjena. Nekateri servisi zahtevajo tudi avtorizacijo uporabnika, tj. preverjanje dodatnih podatkov o članu, kot je kategorija člana (študent, zaposlen na univerzi itd.). Ta avtorizacijska pravila se zapišejo v posebno datoteko, ki se preverja ob prijavi v informacijski servis. O tem, kakšna bodo avtorizacijska pravila, se dogovorita IZUM in knjižnica, ki zagotavlja servis svojim uporabnikom, pri čemer je treba upoštevati licenčne pogoje, dogovorjene s ponudnikom informacijskega servisa. Ob prijavi v informacijski servis se lahko upošteva lokalna politika knjižnice, na osnovi katere se lahko zavrne prijava za določene člane knjižnice, kot so uporabniki, ki imajo v knjižnici dolg ali kakšno drugo omejitev dostopa do e-virov ali drugih knjižničnih storitev. Tudi o teh pogojih se dogovorita IZUM in knjižnica.



Slika 2: Poenostavljena ponazoritev avtentikacijsko-avtorizacijskega mehanizma COBISS preko protokola LDAP

Slika 2 prikazuje poenostavljeno ponazoritev avtentikacijsko-avtorizacijskega mehanizma COBISS preko protokola LDAP. V informacijske servise, ki jih ponujajo IZUM in slovenske knjižnice, se je mogoče prijaviti preko strežnika LDAP, ki komunicira z bazami podatkov o članih knjižnic v sistemu COBISS. Nekatere knjižnice še uporabljajo staro platformo COBISS2/Izposoja, vse več pa jih prehaja na novo platformo COBISS3/Izposoja. Strežnik LDAP je centralna aplikacija prijavnega mehanizma, medtem ko so baze podatkov o članih osnova za pridobivanje podatkov o uporabnikih; ti podatki so potrebni, da se omogočita avtentikacija in avtorizacija prijave v informacijske servise. Nekateri informacijski servisi zahtevajo le avtentikacijo uporabnika (Libroam, Odpiranje vrat, PaperCut, MyPC, Biblos itd.), medtem ko nekateri drugi zahtevajo tudi več podatkov o uporabnikih, tj. avtorizacijo (EZproxy, Metaiskalnik itd.).

Slabost prijavnega sistema LDAP je, da se mora uporabnik v vsak servis prijaviti ponovno, čeprav se je že prijavil v enega izmed njih. Ker informacijski servisi delujejo na različnih platformah in strežnikih, niso medsebojno aplikacijsko povezani, zato mora uporabnik postopek avtentikacije in avtorizacije izvesti vsakič posebej. Da bi se temu ponavljajočemu postopku izognili in zagotovili ne le enako prijavo (angl. *same sign-on*), temveč tudi enotno prijavo (angl. *single sign-on*), je potrebna implementacija aplikativnega modula, ki bi takšno funkcionalnost zagotovil. Še posebej v akademskih in raziskovalnih krogih zahodnega sveta se je uveljavil Shibboleth kot takšen vmesni aplikativni člen med informacijskim servisom in ponudnikom identitete.

SHIBBOLETH

Shibboleth (https://shibboleth.net/) je odprtokodna aplikacija, ki zagotavlja komunikacijo med spletnimi servisi in ponudniki identitet. Zagotavlja enotno prijavo uporabnika. Ko se uporabnik prijavi v prvi informacijski servis z uvedenim modulom Shibboleth, mu je zagotovljena prijava tudi v preostale take servise; uporabniškega imena in gesla mu ni treba ponovno vpisati, saj je svojo identiteto že dokazal ob prijavi v prvi informacijski servis. Za zagotovitev tovrstnega mehanizma prijav mora modul Shibboleth uvesti tako informacijski servis (angl. *Shibboleth SP – Service Provider*) kot tudi ponudnik identitete (angl. *Shibboleth IdP – Identity Provider*).

V IZUM-u smo v tem letu nadgradili obstoječi strežnik LDAP z rešitvijo IdP, ki temelji na tehnologiji SimpleSAMLphp (https://simplesamlphp.org/), ter ga povezali z modulom Shibboleth aplikacije EZproxy in tako uvedli Shibboleth za oddaljen dostop. Naslednji informacijski servis, za katerega smo omogočili takšno prijavo, je Web of Science ponudnika Thomson Reuters. Sledili so mu še informacijski servisi Scopus in ScienceDirect ponudnika Elsevier ter EBSCO.

Ker nekateri ponudniki informacijskih servisov zahtevajo nadgradnjo IdP-ja v federacijo, kar se kaže v metapodatkih, ki si jih ponudnik servisa in ponudnik identitete izmenjata ob medsebojnem povezovanju, smo v IZUM-u izvedli nadgradnjo avtentikacijsko-avtorizacijskega mehanizma LDAP v Federacijo COBISS AAI.

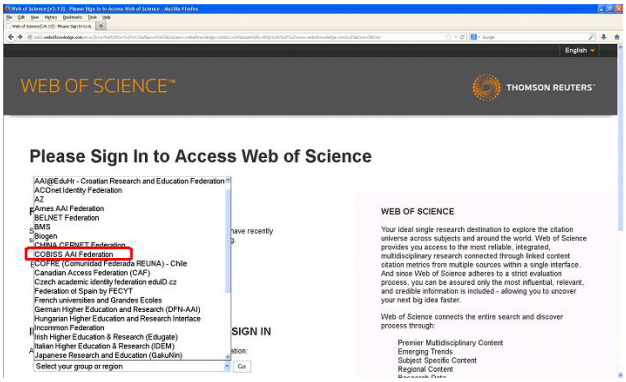
FEDERACIJA COBISS AAI

Federacija COBISS AAI (angl. *authentication and authorization infrastructure*) je rezultat IZUM-ovih avtentikacijsko-avtorizacijskih rešitev in zagotavlja knjižnicam sistema COBISS in njihovim končnim uporabnikom enotno prijavo v informacijske servise. V to federacijo je vključena vsaka knjižnica s podprtim avtomatiziranim segmentom COBISS/Izposoja. Trenutno se sistem uporablja le v Sloveniji, vendar ga IZUM namerava nadgraditi tudi za preostale nacionalne knjižnične informacijske sisteme zunaj Slovenije, ki so povezani v COBISS (mreža COBISS.Net).

Federacija COBISS AAI je naravna nadgradnja sistema, o katerem sta pred kratkim že pisala Boštjan Batič in Davor Šoštarič (2013), saj so ustvarjeni vsi pogoji za medsebojno priznavanje identitet, ki jih imajo uporabniki v svojih knjižnicah. V primeru Federacije COBISS AAI gre za okolje povezanih posameznih organizacij – knjižnic, ki medsebojno že sodelujejo v vzajemnem sistemu COBISS, z AAI pa se sinergija tehnološkega in organizacijskega povezovanja še poveča in razširi na področje prijavnih mehanizmov.

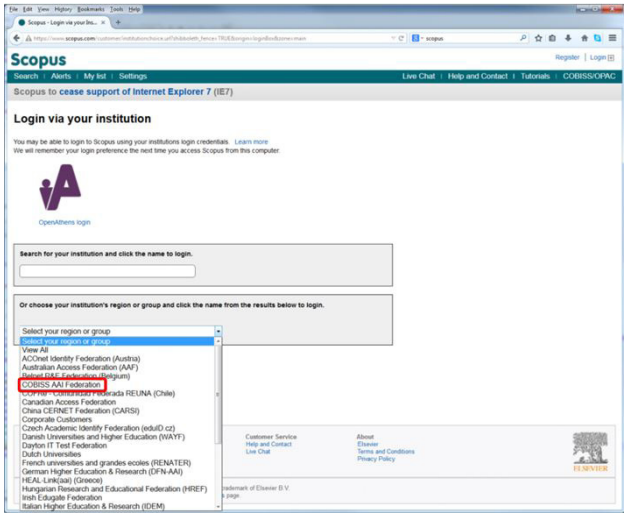
AAI omogoča tudi višji nivo zagotavljanja varstva osebnih podatkov, saj avtentikacijo izvaja ponudnik identitete, v primeru COBISS AAI je to IZUM, medtem ko avtorizacijo izvede ponudnik storitve, ki prejme le podatke o afiliacijskih atributih, potrebnih za avtorizirano prijavo v uporabniški račun institucije v okviru informacijskega servisa. Ponudnik ne prejme osebnih podatkov o uporabniku, kot so e-pošta, ime in priimek uporabnika itd., ter tudi ne podatkov, potrebnih za avtentikacijo (uporabniško ime in geslo). Zagotovljena je uporabniška anonimnost v odnosu do ponudnika storitve.

V letošnjem letu smo v IZUM-u zagotovili možnost prijave za vse članice slovenskega konzorcija Web of Science preko Federacije COBISS AAI, kar prikazuje slika 3. Uporabnik med ponujenimi svetovnimi federacijami AAI izbere Federacijo COBISS AAI, nakar sistem zahteva še vpis uporabniškega imena in gesla, ki ga le-ta uporablja v svoji knjižnici. V primeru pravilnega vnosa bo uporabnik uspešno prijavljen v uporabniški račun matične institucije informacijskega servisa Web of Science, omogočen mu bo dostop do vseh baz podatkov in funkcionalnosti, ki mu jih ponudnik Thomson Reuters omogoča na osnovi formalnega dogovora s knjižnico.

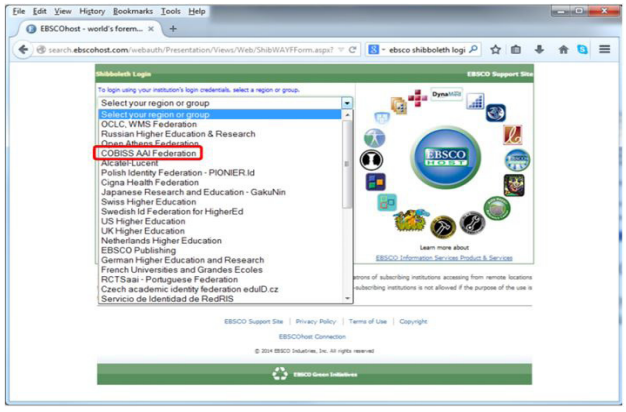


Slika 3: Prijava v informacijski servis Web of Science preko Federacije COBISS AAI (Vir: Thomson Reuters, 2014)

Enaka rešitev je dogovorjena s ponudnikom Elsevier za informacijska servisa Scopus in ScienceDirect ter s ponudnikom EBSCO za njegove informacijske servise. Sliki 4 in 5 prikazujeta prijavo preko Federacije COBISS AAI za omenjena ponudnika.



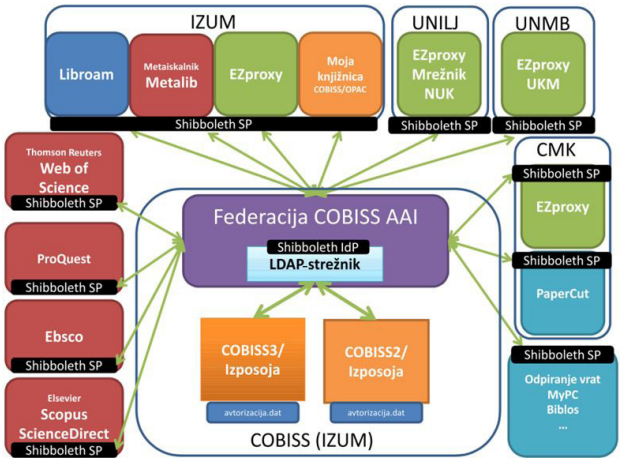
Slika 4: Prijava v informacijska servisa Scopus in Science Direct preko Federacije COBISS AAI (Vir: Elsevier, 2014)



Slika 5: Prijava v informacijske servise ponudnika EBSCO preko Federacije COBISS AAI (Vir: EBSCO, 2014)

IZUM se dogovarja tudi z drugimi svetovnimi ponudniki informacijskih servisov, kot sta npr. ProQuest in Oxford University Press, za vzpostavitev prijavnega mehanizma; pričakovati je, da bo tovrstna avtentikacijsko-avtorizacijska infrastruktura nadomestila druge aplikativne rešitve, ki jih trenutno uporabljajo knjižnice pri omogočanju oddaljenih dostopov do informacijskih servisov. Omogočala bo tudi nadomeščanje klasičnega IP-dostopa, ki je omejen predvsem na dostop le iz prostorov institucij članic, zunaj teh institucij pa dostop ni mogoč.

Slika 6 prikazuje poenostavljeno ponazoritev avtentikacijsko-avtorizacijskega mehanizma preko Federacije COBISS AAI. Cilj IZUM-a je uvesti Shibboleth za vse spletne storitve, ki jih ponujamo, ter preko federacije COBISS AAI zagotoviti in olajšati uporabo spletnih storitev za vse knjižnice, ki so vključene v sistem COBISS. Pred nami so številni izzivi, saj ponudniki informacijskih servisov ponujajo različne pristope in tehnične rešitve povezovanja. V IZUM-u se bomo znali temu prilagoditi in zagotoviti infrastrukturne rešitve.



Slika 6: Poenostavljena ponazoritev avtentikacijsko-avtorizacijskega mehanizma preko Federacije COBISS AAI

FEDERACIJA ARNESAAI

Uporabniki Arnesovih storitev lahko uporabijo za dostop do informacijskih servisov tudi Federacijo ArnesAAI (https://aai.arnes.si/). Arnes upravlja z identitetnimi podatki uporabnikov slovenskega izobraževalnega in raziskovalnega sektorja ter ponuja številne servise, kot so spletne konference VOX, servis Filesender za izmenjavo datotek večjega obsega (do 10 GB) itd. Prijava v te servise temelji na ArnesAAI. Omogočen je tudi dostop do nekaterih informacijskih virov, kot so Web of Science, ProQuest, EBSCO. Organizacije, ki želijo uporabiti to prijavno infrastrukturo, se s svojimi IdP-ji pridružijo Federaciji; če pa nimajo lastne tehnične podpore, lahko uporabijo Arnesovo storitev gostovanja LDAP.

Federacija COBISS AAI je plod uspešnega sodelovanja med IZUM-om in Arnesom za podporo avtentikacijsko-avtorizacijski infrastrukturi tudi za knjižnice in temelji na enaki tehnološki platformi. V prihodnje je pričakovati povezovanje obeh federacij, s čimer bi uporabnikom obeh federacij olajšali prijavo v servise, ki jih uporabljajo pri svojem izobraževalno-raziskovalnem delu.

ZAKLJUČEK

Slovenske knjižnice in IZUM v svojem kooperativnem odnosu omogočajo svojim uporabnikom prijavo v številne informacijske servise, ki jih je pričakovati v prihodnje vse več. Ta prijava temelji na avtentikacijsko-avtorizacijskem mehanizmu COBISS, ki je bil v letošnjem letu nadgrajen v Federacijo COBISS AAI. Federacija predstavlja osnovno prijavno infrastrukturo, ki bo v prihodnje nadomestila dosedanje rešitve in s tem zagotovila

eno izmed pomembnejših prijavnih funkcionalnosti, tj. enotno prijavo. Z drugimi aplikativnimi rešitvami, ki jih načrtujemo v IZUM-u v prihodnjih letih, bomo olajšali in izboljšali izkušnje uporabnikov pri uporabi informacijskih servisov. Med te rešitve sodi možnost povezovanja različnih identitet uporabnikov tako znotraj kot tudi zunaj sistema COBISS (angl. *account linking*), npr. povezovanje z Googlovim ali Twitterjevim računom.

Trenutno se tovrstne rešitve uporabljajo le v Sloveniji, IZUM pa namerava to infrastrukturo ponuditi tudi preostalim članicam sistema COBISS zunaj Slovenije. Nakazuje pa se tudi potreba po povezovanju z drugimi federacijami AAI, kot je npr. Federacija ArnesAAI.

Reference

Batič, B. in Šoštarič, D., 2013. Koncept avtentikacijske in avtorizacijske infrastrukture v sistemu COBISS. *Organizacija znanja*, 18(1–4), pp. 1–6.

EBSCO, 2014. *EBSCOhost*. [online] Dostopno na: http://search.ebscohost.com [20. 8. 2014].

Elsevier, 2014. *Scopus*. [online] Dostopno na: https://www.scopus.com/customer/institutionchoice.url [20. 8. 2014].

Šobot, P., 2013. Povezivanje baza i servisa sistema COBISS.SI sa različitim informacionim servisima. V: Knežević, R., et al. ur. *Zbornik radova X međunarodne konferencije bibliotekara "Informacijska pismenost", 13–15. juni 2013. godine*. Bihać: Kantonalna i univerzitetska biblioteka Bihać. pp. 34–39.

Thomson Reuters, 2014. *Web of Science*. [online] Dostopno na: https://apps.webofknowledge.com [20. 8. 2014].