Temeljem Zaključka Ministarstva znanosti, obrazovanja i športa o prihvaćanju Temeljnih načela Autentikacijske i autorizacijske infrastrukture znanosti i visokog obrazovanja u Republici Hrvatskoj - AAI@EduHr od 27. prosinca 2007. godine, klasa 650-03/07-03/00029, urbroj: 533-05-07-0004 i uz prethodnu suglasnost Ministarstva znanosti, obrazovanja i športa izdanu 5.lipnja 2008. godine, ravnatelj Sveučilišnog računskog centra 11. lipnja 2008. godine donosi

PRAVILNIK O USTROJU

Autentikacijske i autorizacijske infrastrukture znanosti i visokog obrazovanja u Republici Hrvatskoj - AAI@EduHr

(verzija 1.3.1.)

SADRŽAJ

1. OSNOVNI POJMOVI

1.1. Uvodne napomene

Članak 1.

Autentikacijska i autorizacijska infrastruktura znanosti i visokog obrazovanja u Republici Hrvatskoj (dalje u tekstu: **AAI@EduHr**) je infrastrukturni, posrednički sustav čija je temeljna zadaća omogućiti sigurno, pouzdano i efikasno upravljanje elektroničkim identitetima te njihovu uporabu za pristup mrežnim i mrežom dostupnim resursima.

Zapisi u AAI@EduHr predstavljaju temeljne zapise o elektroničkom identitetu fizičkih osoba iz sustava znanosti i visokog obrazovanja u Republici Hrvatskoj. Navedeni zapisi predstavljaju polazište za ostale informacijske i mrežne sustave koji koriste ili se oslanjaju na elektroničke identitete fizičkih osoba iz sustava znanosti i visokog obrazovanja. Takvi informacijski i mrežni sustavi trebaju uvažiti osnovne tehničke i organizacijske zahtjeve AAI@EduHr, te osigurati potrebnu interoperabilnost.

AAI@EduHr utemeljena je na uporabi distribuiranih LDAP imenika, RADIUS poslužitelja i Web servisa te na tehničkim rješenjima razvijenim u Sveučilišnom računskom centru Sveučilišta u Zagrebu (dalje u tekstu: **Srce**) uz puno poštivanje opće prihvaćenih međunarodnih standarda u području gradnje autentikacijskih i autorizacijskih infrastruktura (AAI). Stoga na AAI@EduHr treba gledati i kao na tehnološko rješenje i kao na praktičnu tehničku i organizacijsku realizaciju jedne AAI.

AAI@EduHr nastala je kao rezultat zajedničkog projekta Srca i CARNeta, kojeg je financiralo Ministarstvo znanosti, obrazovanja i športa (dalje u tekstu: MZOŠ), a vodilo Srce. Sustav AAI@EduHr u produkcijskom je radu od 1.3.2006. godine. Brigu o održavanju središnjih usluga kao i daljnjem razvoju te koordinaciji rada cjelokupnog sustava MZOŠ je povjerilo Srcu.

AAI@EduHr povezana je sa sličnim nacionalnim AAI sustavima u Europi i svijetu. AAI@EduHr je spojena u pan-europski roaming sustav pod nazivom eduroam (http://www.eduroam.org) te je sukladno tome i uspostavljeno web sjedište na adresi http://www.eduroam.hr. Uspostavljena je veza sa sustavom eduGAIN (http://www.edugain.org). Srce je od međunarodnih partnera i drugih nacionalnih operatora AAI iz akademske i istraživačke zajednice prepoznato i prihvaćeno kao koordinator nacionalne AAI te nositelj eduroam aktivnosti u Hrvatskoj.

Članak 2.

Znak (logotip) AAI@EduHr je:

Članak 3.

Službeno web sjedište AAI@EduHr nalazi se na adresi http://www.aaiedu.hr/

Službeno web sjedište informacijski i tehnički održava Koordinator AAI@EduHr.

Na službenom web sjedištu objavljuju se službeni dokumenti, činjenice i novosti vezane uz AAI@EduHr. Informacije se objavljuju na hrvatskom i engleskom jeziku.

Članak 4.

Ovim se **Pravilnikom** uređuje ustroj AAI@EduHr kroz definiranje organizacijskog modela, prava i obveza svih subjekata te operativnih procedura kojih su se ti subjekti dužni pridržavati.

1.2. Općeniti koncept AAI

Članak 5.

Koncept AAI nastao je kao rezultat rješavanja problema inter-institucionalne autentikacije i autorizacije (AA) korisnika s ciljem da korisniku osigura jednostavan, uniforman i siguran mehanizam pristupa mreži i mrežnim resursima.

U svakoj AAI postoje tri osnovna subjekta za čije ponašanje je potrebno utvrditi prava i obveze:

- matična ustanova (davatelj elektroničkog identiteta),
- vlasnik resursa (davatelj usluge),
- krajnji korisnik.

Svoja prava u okviru AAI korisnik ostvaruje temeljem svog elektroničkog identiteta. Elektronički identitet je skup podataka o pojedincu koji se koristi za potrebe provjere identiteta (autentikacija) i prava pristupa (autorizacija). Pamti se u naročitoj bazi podataka koju zovemo imenik.

Temeljni proces u AAI čine tri osnovne akcije koje se odvijaju između korisnika, njegove matične ustanove i vlasnika resursa:

1) Autentikacija korisnika koju obavlja njegova matična ustanova. Obavlja se temeljem elektroničkog identiteta kojeg je korisniku izdala upravo ta ustanova
2) Prijenos korisnikovih autorizacijskih atributa od matične ustanove do ustanove - vlasnika resursa. Skup atributa koji se prenose mora biti konfigurabilan kako bi se ispunili zahtjevi vlasnika resursa, ali i štitila privatnost korisnika.
3) Autorizacija odnosno odluka o pristupu resursu koju donosi vlasnik resursa.

AAI su u pravilu složeni sustavi u kojima postoje i bitne središnje usluge. Kako bi se osiguralo funkcioniranje središnjih usluga te koordinirao njen rad potrebno je da svaka AAI ima svog koordinatora odnosno ustanovu koja obavlja navedene poslove održavanja i razvoja.

2. ARHITEKTURA AAI@EDUHR

2.1. Tehnički opis AAI@EduHr

Članak 6.

AAI@EduHr svoje polazište koncepcijski ima u distribuiranom sustavu imenika utemeljenih na LDAP standardu. Konkretna implementacija LDAP imenika u AAI@EduHr temelji se na **hrEduPerson i HrEduOrg imeničkim shemama** kojima se opisuju osobe odnosno matične ustanove u sustavu.

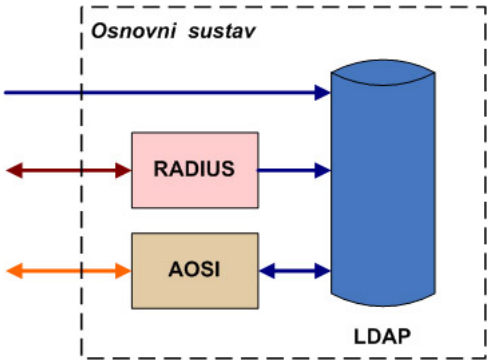
Nadležnost nad imeničkim podacima o fizičkim i pravnim osobama, te informacijskim i drugim resursima imaju njihove matične ustanove. Te ustanove, kao jedine mjerodavne, trebaju kroz provođenje definiranih pravila i procedura osigurati informacijsku potpunost, konzistentnost i vjerodostojnost sadržaja imenika.

Konkretna prava pristupa i/ili uporabe određuju vlasnici pojedinih resursa kroz pristupne mehanizme, kompatibilne, u smislu definiranih standarda i protokola s AAI@EduHr.

Članak 7.

AAI@EduHr komponentu sustava (vidjeti sliku 1.) na matičnoj ustanovi čine:

- LDAP imenik u kojem su pohranjeni podaci o elektroničkim identitetima,
- RADIUS poslužitelj (primarno namjenjen autentikaciji),
- AOSI (aplikacija za održavanje sadržaja imenika) web servis za dohvat podataka i održavanje LDAP imenika.



Slika 1. – AAI@EduHr komponenta sustava na matičnoj ustanovi

LDAP imeniku matične ustanove pristupa se putem odgovarajućeg RADIUS poslužitelja ili AOSI web servisa.

Sustav AOSI je zamišljen i razvijen po modelu klijent-poslužitelj, kao otvoren, modularan i lako nadogradiv odnosno uskladiv s novim AAI tehnologijama i standardima. Oslanja se na tehnologiju Web servisa.

Klijentskom komponentom sustava AOSI omogućeno je pouzdano, sigurno i efikasno upravljanje elektroničkim identitetima.

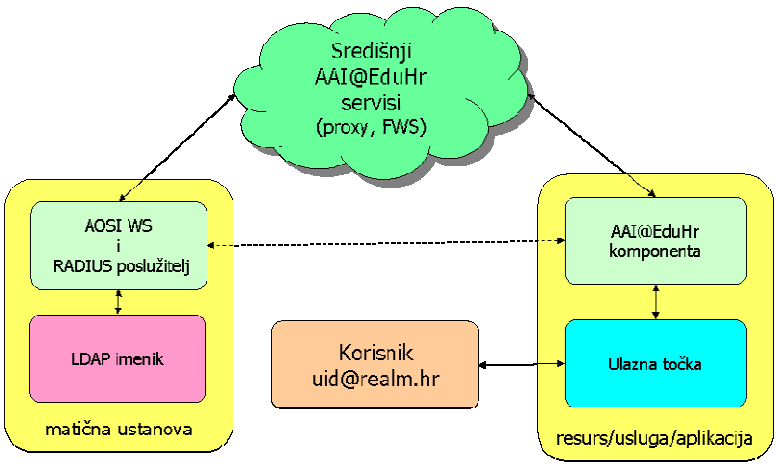
Članak 8.

Uloga je središnjih servisa AAI@EduHr osigurati jednostavno, pouzdano i sigurno provođenje procesa autentikacije i autorizacije korisnika. Proces inicira korisnik prilikom pristupa nekom resursu koji je usklađen s AAI@EduHr standardom. AA komponenta resursa posredstvom središnjih servisa kontaktira AA komponentu na matičnoj ustanovi. Provodi se proces autentikacije odnosno provjere identiteta, a zatim i autorizacije na temelju podataka vezanih uz elektronički identitet korisnika.

Središnji servisi u sustavu AAI@EduHr su:

- **središnji RADIUS proxy poslužitelj**: primarno namjenjen autentikaciji uz korištenje RADIUS protokola te stoga posebno primjenjiv u AA procesu kod pristupa mreži
- **federacijski web servis (FWS):** pruža mogućnost autentikacije i autorizacije korisnika uz uporabu HTTPS/SOAP protokola; posebno primjenjiv u AA procesu mrežnim aplikacijama koje rabe HTTP protokol.

Arhitektura sustava AAI@EduHr prikazana je na slici 2.



Slika 2. – Arhitektura sustava AAI@EduHr

2.2. Imeničke sheme sustava AAI@EduHr

Članak 9.

hrEduPerson i HrEduOrg (dalje u tekstu **hrEdu sheme**) standardne su imeničke sheme sustava AAI@EduHr.

Shema hrEduPerson rabi se za podatke o osobama, a shema hrEduOrg shema za podatke o ustanovama.

Članak 10.

Atributi u hrEdu shemama mogu biti obavezni ili opcionalni, u zavisnosti od čega ih mora ili može imati svaki zapis u LDAP imeniku.

Gledajući učestalost pojavljivanja vrijednosti pojedinih atributa, za pojedini elektronički identitet oni mogu biti jednostruke ili višestruke vrijednosti.

Članak 11.

Da bi zapis u LDAP imeniku bio ispravan mora imati popunjene točne vrijednosti svih obaveznih atributa navedenih u hrEdu shemi.

Članak 12.

Davatelj usluge može jedan ili više opcionalnih atributa proglasiti obaveznim za korisnike svoje usluge te vrijednosti tih atributa rabiti u procesu autorizacije korisnika.

Članak 13.

Definicije hrEdu shema javno su dostupne putem registra imeničkih shema (http://schema.aaiedu.hr). Registar je referentna točka za imeničke sheme u sustavu AAI@EduHr te nudi sve potrebne podatke o imeničkim shemama i njihovoj implementaciji.

Članak 14.

hrEdu sheme podložne su promjenama i svaki subjekt u sustavu AAI@EduHr ima pravo predlagati promjenu postojećih atributa ili dodavanje novih.

O promjenama hrEdu shema odlučuje Koordinator AAI@EduHr.

Koordinator AAI@EduHr objavljuje promjene shema putem registra imeničkih shema najmanje 2 mjeseca prije njihovog stupanja na snagu. Koordinator AAI@EduHr je dužan osigurati potrebne upute i alate koji će omogućiti pouzdanu migraciju podatka iz stare u novu imeničku shemu.

2.3. Središnje usluge sustava AAI@EduHr

Članak 15.

Sve središnje usluge sustava AAI@EduHr udomljuje i održava Koordinator AAI@EduHr.

Pretpostavka kvalitetnog rada AAI@EduHr je i postojanje nacionalne akademske i istraživačke računalno-komunikacijske mreže CARNet.

Članak 16.

Središnje usluge sustava AAI@EduHr čine:

- **središnji servisi AAI@EduHr:**
  - RADIUS proxy poslužitelji
  - FWS poslužitelji.

  Postojeća konfiguracija s višestrukim središnjim poslužiteljima omogućuje load balancing i backup funkcije čime je postignuta veća pouzdanost usluge;
- **središnji informacijski servis**, odnosno web poslužitelji na adresama http://www.aaiedu.hr i http://www.eduroam.hr;
- **registar imeničkih shema** (http://schema.aaiedu.hr). Funkcija je registra da bude referentna točka za imeničke sheme u sustavu AAI@EduHr te nudi sve potrebne podatke o imeničkim shemama i njihovoj implementaciji;
- **registar matičnih ustanova** (http://www.aaiedu.hr/sastavnice/) koji ima funkciju osigurati ažurne podatke o matičnim ustanovama nužne za funkcioniranje cjelokupne infrastrukture;
- **registar davatelja usluga** (https://www.aaiedu.hr/aairr/) koji ima funkciju osigurati ažurne podatke o davateljima usluga nužne za funkcioniranje cjelokupne infrastrukture;
- **sustav nadzora AAI@EduHr** (http://www.aaiedu.hr/status/) koji ima zadaću osigurati informacije o radu svih elemenata sustava;
- **LDAP/RADIUS hosting usluga** (https://hosting.aaiedu.hr/) kojom se omogućuje udomljavanje AAI@EduHr komponente za one matične ustanove koje nisu u mogućnosti samostalno osigurati potrebne tehničke preduvjete;
- **centar potpore** koji nudi:
  - www.aaiedu.hr kao portal za podršku svim kategorijama korisnika,
  - seminare za matične ustanove i davatelje usluga,
  - savjetodavnu pomoć pri uporabi ili implementaciji AAI tehnologija,
  - mailing liste za održavatelje na matičnim ustanovama (admin-l@aaiedu.hr) i razvojne inženjere (develop-l@aaiedu.hr);
- **repozitorij programske podrške** dostupan putem ftp poslužitelja Srca (ftp://ftp.srce.hr) putem kojeg je organizirana distribucija programskih paketa vezanih uz AAI@EduHr. Radi se prije svega o LDAP i RADIUS poslužitelju, AOSI web servisu i web klijentu, ali i nizu drugih programskih rješenja namijenjenih za uporabu na matičnim ustanovama ili u funkciji davatelja resursa u sustavu. Paketi su napravljeni po Linux/debian standardu, a repozitorij se stalno nadopunjuje sukladno uočenim potrebama.
- **poslužitelj javnih PGP ključeva** s pratećim web sjedištem (http://pks.aaiedu.hr/) putem kojeg je omogućeno publiciranje i pronalaženje PBG javnih ključeva.

3. ORGANIZACIJA AAI@EDUHR

3.1. Organizacijski model

Članak 17.

AAI@EduHr organizirana je kao **federacija ustanova članica**.

Ustanove članice su **matične ustanove** (davatelji elektroničkih identiteta) koje istodobno mogu, ali i ne moraju biti davatelji usluga.

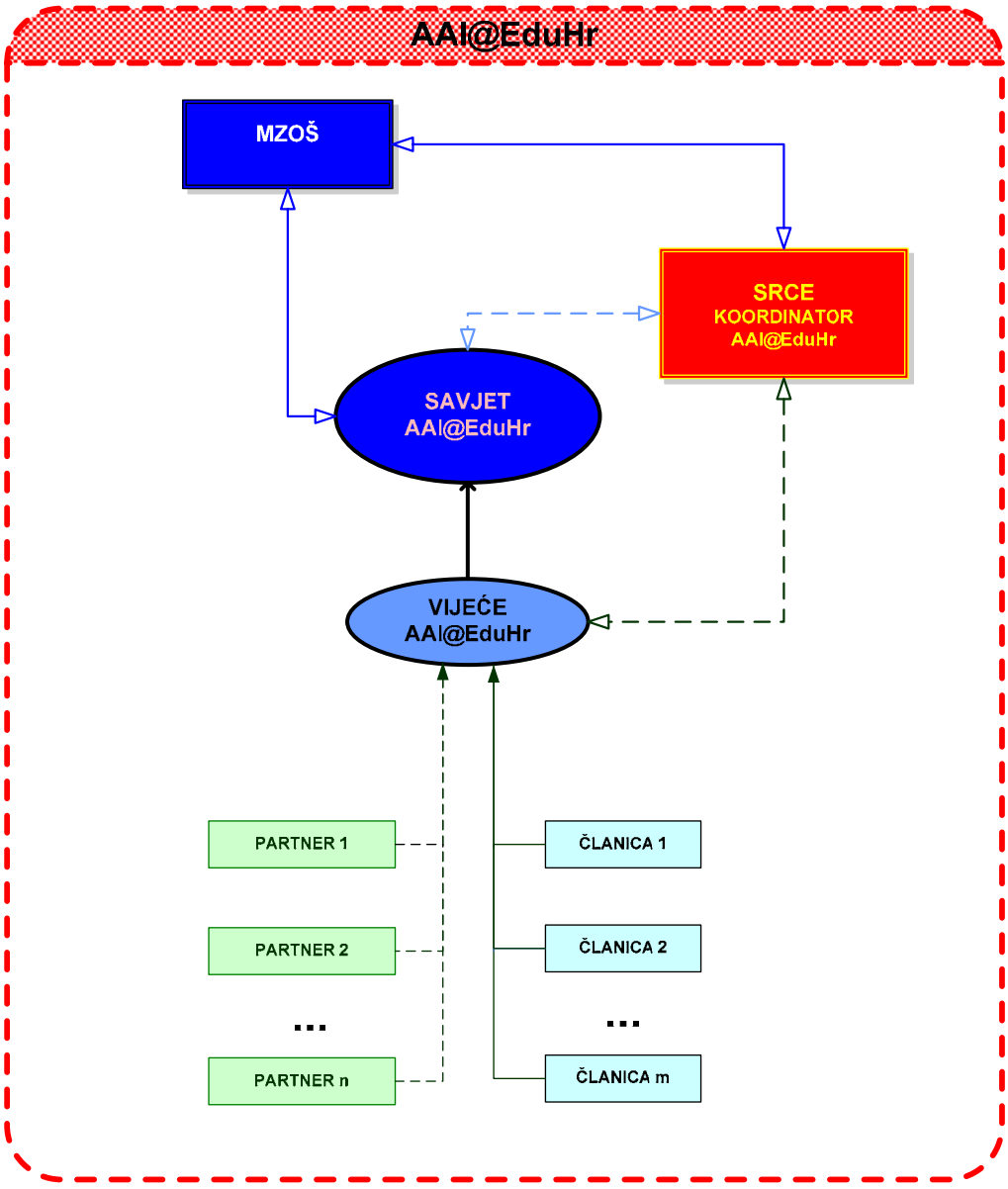
Ustanove koje se pojavljuju isključivo u ulozi davatelja usluge i ne mogu imati status matične ustanove nazivamo (vanjskim) **partnerima** AAI@EduHr federacije.

Poslove koordinacije rada AAI@EduHr te razvoja i održavanja središnjih usluga AAI@EduHr obavlja **Koordinator AAI@EduHr**. Rad Koordinatora AAI@EduHr nadgleda MZOŠ.

Vijeće AAI@EduHr ima savjetodavnu ulogu i prenosi Koordinatoru AAI@EduHr potrebe odnosno prijedloge članica za daljnjim razvojem te istodobno potiče i pomaže pridržavanje svih utvrđenih organizacijskih i tehničkih standarda u AAI@EduHr.

Savjet AAI@EduHr sudjeluje u upravljanju sustavom AAI@EduHr u skladu s ovlastima iz ovoga Pravilnika (vidi članke 37. i 38.).

Organizacijski model AAI@EduHr prikazan je na slici 3.



Slika 3. - Organizacijski model AAI@EduHr

AAI@EduHr osigurava:

- korisnicima, pojedincima: jednostavno, sigurno i pouzdano korištenje svih usluga u sustavu AAI@EduHr uz pomoć jedinstvenog elektroničkog identiteta dobivenog na matičnoj ustanovi;
- matičnim ustanovama (davateljima elektroničkih identiteta): sigurno, pouzdano i efikasno upravljanje elektroničkim identitetima svojih djelatnika, suradnika i studenata kojima je bitno olakšano korištenje različitih mrežnih i mrežom dostupnih resursa, uz minimalnu administraciju;
- davateljima usluga (resursa): veću dostupnost i vidljivost usluge uz pojednostavljenu administraciju i standardiziran proces autentikacije i autorizacije korisnika.

3.2. Ministarstvo znanosti, obrazovanja i športa (MZOŠ)

Članak 18.

MZOŠ upravlja s AAI@EduHr, putem Savjeta AAI@EduHr, kojeg imenuje ministar znanosti, obrazovanja i športa.

MZOŠ osigurava sredstva potrebna za rad AAI@EduHr sukladno usvojenom godišnjem planu, a prema mogućnostima državnog proračuna i MZOŠ.

3.3. Koordinator AAI@EduHr

Članak 19.

Koordinator AAI@EduHr (dalje u tekstu: ***Koordinator***) predstavlja i zastupa interese AAI@EduHr u pravnom prometu i međunarodnim odnosima, operativni je nositelj AAI@EduHr i osigurava planiranje, izgradnju, održavanje i svakodnevno funkcioniranje AAI@EduHr.

Koordinator AAI@EduHr je Srce.

Zadaća je Koordinatora AAI@EduHr:

- donositi Pravilnik i izmjene Pravilnika o ustroju AAI@EduHr uz prethodnu suglasnost MZOŠ
- donositi tehnička i organizacijska pravila, procedure i preporuke AAI@EduHr
- odlučivati o statusu članica i partnera
- osigurati pouzdan i kvalitetan rad svih središnjih usluga AAI@EduHr navedenih u članku 16.
- nadzirati i koordinirati rad cjelokupne AAI@EduHr
- u ime i za račun članica uspostavljati veze s drugim AA sustavima
- predstavljati AAI@EduHr u nacionalnim i međunarodnim odnosima.

Koordinator u ime i za račun članica uspostavlja veze s drugim AAI federacijama u zemlji i svijetu. O uspostavljenim je kontaktima i dogovorima dužan izvijestiti Savjet AAI@EduHr.

Koordinator o svom radu podnosi godišnje izvješće Savjetu i Vijeću korisnika AAI@EduHr te MZOŠ.

Koordinator je dužan očitovati se o svim prijedlozima Savjeta i Vijeća.

Članak 20.

Ravnatelj Srca iz redova zaposlenika Srca imenuje voditelja AAI@EduHr, osobu koja operativno koordinira izvršavanje poslova iz nadležnosti Koordinatora te vodi odgovarajući tim.

3.4. Članice AAI@EduHr

Članak 21.

Članice AAI@EduHr su matične ustanove koje istodobno mogu, ali i ne moraju biti i davatelji usluga.

Članice delegiraju svoje predstavnike u Vijeće AAI@EduHr.

Članak 22.

Status članice može se promijeniti na vlastiti zahtjev ili odlukom Koordinatora.

Na odluku Koordinatora moguća je žalba Savjetu AAI@EduHr. Odluka Savjeta je konačna.

Članak 23.

Matičnom ustanovom, a time i članicom AAI@EduHr može postati svaka pravna osoba iz sustava znanosti i visokog obrazovanja koja je:

- ili upisana u Upisnik visokih učilišta pri MZOŠ
- ili upisana u Upisnik znanstvenih organizacija pri MZOŠ
- ili ima status punopravne ili pridružene članice Hrvatske akademske i istraživačke mreže CARNet,

a koja pisanim putem potvrdi da će se pridržavati odredbi ovog Pravilnika te obavljati poslove matične ustanove (vidi 3.6.).

Za subjekte iz stavka 1. ovoga članka odluku o članstvu donosi Koordinator.

Drugi subjekti iz sustava znanosti i obrazovanja status matične ustanove mogu steći samo posebnom odlukom Savjeta AAI@EduHr.

Subjekti iz sustava osnovnog i srednjeg školstva članstvo u AAI@EduHr ne ostvaruju pojedinačno, već zajednički putem središnjeg sustava kojeg razvija i održava CARNet.

O eventualnim izuzetcima od odredbi iz prethodnih stavaka ovoga članka odlučuje Savjet AAI@EduHr.

Članak 24.

Subjekt koji želi steći status članice AAI@EduHr podnosi Koordinatoru zahtjev na odgovarajućem obrascu. Obrazac propisuje Koordinator.

Odluku o zahtjevu subjekta iz stavka 1., članka 21. Koordinator donosi u roku od 8 dana od dana zaprimanja zahtjeva.

Podnositelj zahtjeva može na odluku Koordinatora uložiti žalbu Savjetu AAI@EduHr u roku od 15 dana od dana zaprimanja odluke. Žalba se dostavlja Koordinatoru u pisanom obliku.

Zahtjev subjekta iz stavka 3. članka 21. Koordinator je dužan u roku od 2 dana proslijediti na odlučivanje Savjetu AAI@EduHr.

Savjet AAI@EduHr donosi odluku o zahtjevu ili žalbi u roku od 30 dana od dana kada je Koordinator zaprimio zahtjev ili žalbu. Odluka koju donosi Savjet AAI@EduHr je konačna.

3.5. Partneri AAI@EduHr

Članak 25.

Partneri AAI@EduHr su pravne osobe koje su isključivo davatelji usluga u sustavu AAI@EduHr. To su u pravilu ustanove izvan sustava MZOŠ, a mogu biti i međunarodne pravne osobe.

Partneri AAI@EduHr mogu delegirati svoje predstavnike u Vijeće AAI@EduHr.

Partneri AAI@EduHr imaju ista prava i obveze davatelja usluga (vidi 3.7).

Članak 26.

Subjekt koji želi steći status partnera AAI@EduHr podnosi Koordinatoru zahtjev na odgovarajućem obrascu. Obrazac propisuje Koordinator.

Koordinator donosi odluku o zahtjevu u roku od 8 dana od dana zaprimanja zahtjeva.

Podnositelj zahtjeva može na odluku Koordinatora uložiti žalbu Savjetu AAI@EduHr u roku od 15 dana od dana zaprimanja odluke. Žalba se dostavlja Koordinatoru u pisanom obliku.

Savjet AAI@EduHr donosi odluku o žalbi u roku od 30 dana od dana kada je Koordinator zaprimio žalbu. Odluka o žalbi koju donosi Savjet AAI@EduHr je konačna.

3.6. Prava i obveze matičnih ustanova

Članak 27.

Matična ustanova dužna je imenovati osobe odgovorne za tehničku ispravnost i informacijsku pouzdanost svoga LDAP imenika i prateće programske podrške iz članka 7. te o tome izvijestiti Koordinatora. Imenovanje se obavlja pisanim putem na obrascu kojeg propisuje Koordinator.

Odgovorne osobe iz stavka 1. ovoga članka dužne su održavati podatke o matičnoj ustanovi u registru matičnih ustanova kojeg održava Koordinator.

Članak 28.

Matična ustanova dužna je osigurati pouzdan rad i tehničku ispravnost svoje komponente sustava AAI@EduHr (vidi članak 7.) te omogućiti Koordinatoru nadzor rada putem odgovarajuće programske podrške.

Članak 29.

Matična ustanova je vlasnik svog LDAP imenika i odgovorna je za njegovu informacijsku pouzdanost i cjelovitost.

Matična ustanova dodjeljuje elektroničke identitete fizičkim osobama iz kruga svojih djelatnika, suradnika i studenata te ostalih fizičkih osoba za koje se može nedvojbeno utvrditi povezanost s ustanovom, poštujući pri tome pravila vezana uz hrEdu imeničke sheme (vidi 2.2.).

Elektroničke identitete dodjeljuju i održavaju isključivo osobe koje ovlasti matična ustanova. Preporuka je da te ovlaštene osobe budu djelatnici referade ili sličnih službi koje su i inače zadužene za prikupljanje osobnih podataka, to jest službe koje izdaju uvjerenja o statusu osoba i raspolažu s relevantnim podacima, te su utoliko ovlaštene na temelju tih podataka dodjeljivati korisniku pojedini status.

Prije prikupljanja osobnih podataka ovlaštene osobe matične ustanove dužne su informirati korisnika kojeg registriraju o svrsi obrade kojoj su podaci namijenjeni, mogućim korisnicima podataka kao i mogućim posljedicama uskrate podataka te zatražiti njegov pisani pristanak za upisivanje u imenik ustanove.

Matična ustanova dužna je voditi evidenciju o dodijeljenim elektroničkim identitetima.

Ovlaštene osobe matične ustanove dužne su, tijekom procesa registracije korisnika, ustanoviti točnost podataka na osnovu kojih kreiraju elektronički identitet i na siguran način, nedostupan trećim osobama, dostaviti korisniku podatke pomoću kojih dokazuje svoj elektronički identitet.

Ovlaštene osobe matične ustanove dužne su se brinuti o ažurnosti podataka u imeniku.

Matična ustanova je dužna ukloniti odgovarajući elektronički identitet iz svog imenika ako fizička osoba izgubi status na temelju kojeg je stekla pravo na elektronički identitet.

Matična ustanova mora poduzeti sve mjere unutar svojih mogućnosti i nadležnosti da bi osigurala pristup osobnim podacima pohranjenima unutar AAI@EduHr sustava samo ovlaštenim osobama odnosno kroz sustav AAI@EduHr.

U slučaju sigurnosnog incidenta, a na pisani zahtjev ovlaštenog tijela za praćenje sigurnosnih incidenata, matična ustanova dužna je surađivati u svrhu otkrivanja stvarnog identiteta počinitelja sigurnosnog incidenta.

Matična ustanova dužna je omogućiti Koordinatoru nadzor nad procesom dodjele i održavanja elektroničkih identiteta.

Matična ustanova ima pravo proširiti hrEdu sheme za svoju lokalnu upotrebu, ne narušavajući pri tome njihovu funkcionalnost. Matična ustanova može neki od opcionalnih atributa proglasiti obaveznim u svom imeniku.

Matična ustanova dužna je pri izvršenju obveza iz ovog članka, u potpunosti poštovati propise koji reguliraju zaštitu osobnih podataka.

Članak 30.

Ukoliko Koordinator AAI@EduHr utvrdi da matična ustanova krši odredbe ovog Pravilnika dužan ju je upozoriti.

U slučaju ozbiljnijeg ili trajnijeg kršenja Pravilnika Koordinator može privremeno ili trajno ukinuti status ustanovi.

3.7. Prava i obveze davatelja usluga

Članak 31.

Davateljem usluge može postati svaka pravna osoba koja pisanim putem potvrdi da će se pridržavati odredbi ovog Pravilnika te pružati jednu ili više usluga korisnicima oslanjajući se na sustav AAI@EduHr u procesu autentikacije i autorizacije.

Davatelj usluge koji nije ujedno i matična ustanova, ne može imati status članice AAI@EduHr. Takav davatelj usluge ima status partnera AAI@EduHr (vidi 3.5.).

Članak 32.

Davatelj usluge dužan je imenovati odgovornu osobu za pitanja korištenja AAI@EduHr te o tome izvijestiti Koordinatora. Imenovanje se obavlja pisanim putem na obrascu kojeg propisuje Koordinator.

Odgovorna osoba iz stavka 1. ovoga članka dužna je održavati podatke o davatelju usluge u registru davatelja usluga kojeg održava Koordinator.

Članak 33.

Davatelj usluge određuje tko i na koji način može koristiti njegove usluge.

Davatelj usluge rabi sustav AAI@EduHr za autentikaciju i autorizaciju korisnika.

Za potrebe autorizacije korisnika davatelj usluge može odabrati bilo koji od atributa iz hrEdu shema te ga proglasiti obaveznim za svoje korisnike.

Članak 34.

Davatelj usluge dužan je, uz obrazloženje, prijaviti putem registra davatelja usluga sve atribute iz HrEdu shema koje želi koristiti u procesu autentikacije i autorizacije za pristup svojim uslugama.

Ukoliko davatelj usluge nudi više usluga mora prijaviti svaku od njih zasebno.

Davatelj usluge dužan je koristiti dostupne sigurnosne mehanizme te slijediti odgovarajuće preporuke Koordinatora.

Davatelj usluge ne smije pohranjivati vrijednosti atributa koje su korištene u procesu autentikacije i autorizacije osim za potrebe kreiranja logova pri čemu mora jasno navesti njihovu svrhu kreiranja i vrijeme čuvanja.

Davatelj usluge sustav AAI@EduHr smije rabiti samo u svrhu i na način koji je prijavio Koordinatoru putem registra davatelja usluga.

Davatelj usluge dužan je čuvati privatnost korisnika iz sustava AAI@EduHr. Podatke koje su mu dostupni putem AAI@EduHr ne smije dati na uporabu trećim osobama.

Članak 35.

Ukoliko Koordinator utvrdi da davatelj usluge krši odredbe ovog Pravilnika dužan ga je upozoriti.

U slučaju ozbiljnijeg ili trajnijeg kršenja Pravilnika Koordinator može privremeno ili trajno ukinuti status davatelja usluge. Ukidanje statusa može biti u cijelosti (za sve usluge) ili samo djelomično (samo za uslugu koju je davatelj pružao kršeći odredbe ovog Pravilnika).

Na odluku iz stavka 2. ovoga članka davatelj usluge može se žaliti Savjetu AAI@EduHr. Žalba se podnosi pisanim putem. Odluka Savjeta AAI@EduHr je konačna.

3.8. Krajnji korisnici AAI@EduHr

Članak 36.

Krajnjim korisnicima AAI@EduHr smatraju se sve fizičke osobe koje posjeduju valjani elektronički identitet izdan od matične ustanove iz sustava AAI@EduHr. Krajnji korisnici mogu rabiti sve usluge u sustavu pod uvjetom da ispunjavaju uvjete i poštuju pravila koja postavi davatelj usluge.

Krajnji korisnici AAI@EduHr u pravilu posjeduju samo jedan elektronički identitet u sustavu AAI@EduHr.

Iznimno se krajnjim korisnicima usluga u sustavu AAI@EduHr mogu smatrati i one fizičke osobe koje posjeduju elektronički identitet izdan od neke druge AAI federacije s kojom je, u ime AAI@EduHr, Koordinator AAI@EduHr uspostavio suradnju.

Članak 37.

Korisnik ima mogućnost samostalnog upravljanja vrijednostima određenih atributa u skladu s odlukama Koordinatora AAI@EduHr sustava i njegove matične ustanove. Korisnik je odgovoran za točnost i ažurnost podataka koji su na opisani način stavljeni u njegovu nadležnost.

U svrhu sticanja elektroničkog identiteta, korisnik je dužan dati točne podatke matičnoj ustanovi.

Korisnik je dužan čuvati povjerljivost podataka kojima dokazuje svoj identitet (zaporka), te ne ustupati iste drugim osobama.

U slučaju kompromitiranja podataka kojima dokazuje svoj identitet korisnik je dužan o tome informirati matičnu ustanovu.

U slučaju promjene ili uočavanja netočnih osobnih podataka čije je održavanje u nadležnosti matične ustanove, korisnik je obavezan izvijestiti odgovornu osobu na matičnoj ustanovi.

Korisnik ima pravo zatražiti od matične ustanove popis podataka, koje o njemu prikuplja matična ustanova za potrebe zapisa u imeniku.

Korisnik ima pravo od Koordinatora zatražiti popis davatelja usluga u sustavu AAI@EduHr kao i popis atributa koje davatelji usluga koriste prilikom autentikacije i autorizacije korisnika.

Korisnik ima pravo zatražiti da se davateljima usluga uskrati pristup pojedinim atributima odnosno podacima koji se čuvaju kao dio njegovog zapisa u imeniku matične ustanove.

Korisnik ima pravo od matične ustanove pisanim putem zatražiti da se izbriše njegov elektronički identitet iz imenika.

3.9. Vijeće i Savjet AAI@EduHr

Članak 38.

Vijeće AAI@EduHr čine predstavnici članica i partnera AAI@EduHr (jedan predstavnik po ustanovi), te po jedan predstavnik MZOŠ i Koordinatora AAI@EduHr.

Vijeće raspravlja o potrebama članica i partnera AAI@EduHr te o izvještajima o uporabi i planovima razvoja AAI@EduHr.

Vijeće iz redova svojih članova jednom u dvije godine bira predsjedavajućeg Vijeća, te 3 predstavnika u Savjet AAI@EduHr.

Sjednice Vijeća korisnika održavaju se najmanje jednom godišnje.

Prema potrebi sjednica se može održati i elektronički, putem videokonferencijskog sustava i/ili putem elektroničke pošte.

Sjednice Vijeća saziva predsjednik Vijeća, na vlastitu inicijativu, na inicijativu dvadeset članova vijeća, na inicijativu predsjednika Savjeta ili na inicijativu Koordinatora.

Vijeće odluke donosi većinom glasova svih verificiranih članova Vijeća koji su pristupili glasovanju.

Članak 39.

Savjet AAI@EduHr broji 9 članova i čine ga:

- dva predstavnika MZOŠ
- predstavnik Rektorskog zbora
- predstavnik Srca - Koordinatora AAI@EduHr
- predstavnik Hrvatske akademske i istraživačke mreže CARNet
- predstavnik Hrvatske nacionalne grid infrastrukture (CRO NGI)
- te 3 predstavnika koje bira Vijeće AAI@EduHr (od kojih je jedan obvezno predstavnik iz redova veleučilišta i visokih škola, a drugi iz redova javnih instituta).

MZOŠ imenuje članove Savjeta AAI@EduHr.

Savjet AAI@EduHr djeluje u užem sastavu sve dok se ne formira Vijeće AAI@EduHr.

Mandat Savjeta traje 2 godine.

Savjet bira predsjednika iz redova svojih članova.

Savjet:

- raspravlja i prihvaća strateške smjernice razvoja AAI@EduHr
- raspravlja i prihvaća strateške smjernice za međunarodnu suradnju u području AAI
- raspravlja i daje mišljenje o godišnjem planu rada
- raspravlja i daje mišljenje o godišnjem izvještaju o radu i uporabi AAI@EduHr
- odlučuje o žalbama vezanim uz odluke o statusu članica i partnera koje je donio Koordinator.

Članak 40.

Sjednice Savjeta AAI@EduHr održavaju se najmanje dva puta godišnje.

Prema potrebi sjednica se može održati i elektronički, putem videokonferencijskog sustava i/ili putem elektroničke pošte.

Sjednice Savjeta saziva predsjednik Savjeta, na vlastitu inicijativu, na inicijativu tri člana Savjeta ili na inicijativu Koordinatora.

Verificiranim članom Savjeta se smatra osoba za koju je na sjednici Savjeta utvrđeno da postoji odluka MZOŠ o imenovanju.

Savjet odluke donosi većinom glasova svih verificiranih članova Savjeta.

Sjednicama Savjeta bez prava glasa prisustvuje Voditelj AAI@EduHr.

4. FINANCIRANJE

Članak 41.

Operativno funkcioniranje svih središnjih usluga AAI@EduHr financira se iz državnog proračuna.

Na prijedlog Koordinatora MZOŠ osigurava dodatna sredstva za razvoj i unapređenje AAI@EduHr.

Održavanje AAI@EduHr komponenti u nadležnosti članica i partnera financiraju same članice i partneri.

Članice i partneri pokrivaju i sve ostale troškove koji su za njih proizašli iz sudjelovanja u sustavu AAI@EduHr.

5. ODGOVORNOST

Članak 42.

Koordinator, članice i partneri AAI@EduHr dužni su se s osobnim podacima, to jest zbirkama osobnih podataka ponašati u skladu s važećim zakonima Republike Hrvatske.

Matične ustanove vlasnici su LDAP imenika.

Davatelji usluga provode unaprijed precizno definirane obrade nad podacima u LDAP imenicima.

Koordinator djeluje kao posrednik između matične ustanove i davatelja usluge te u tom smislu nije odgovoran za ispravnost podataka koji se nalaze u imeniku matične ustanove niti za eventualnu zloporabu podataka koju počini bilo matična ustanova bilo davatelj usluga.

6. ZAVRŠNE ODREDBE

Članak 43.

Ovaj Pravilnik stupa na snagu danom donošenja.

Članak 44.

Izmjene ovog Pravilnika donosi ravnatelj Srca uz prethodnu suglasnost MZOŠ.

Za tumačenje ovog Pravilnika nadležan je Koordinator.

Članak 45.

Ustanove koje u trenutku donošenja ovog Pravilnika obavljaju poslove matične ustanove ili davatelja usluge moraju u roku od 30 dana dostaviti Koordinatoru zahtjeve za sticanje odgovarajućeg statusa.

Ukoliko to ne učine, a nastave pružati usluge odnosno dodjeljivati elektroničke identitete, smatrat će se da su prihvatile ovaj Pravilnik. Koordinator međutim može pokrenuti postupak ukidanja njihovog statusa.

Članak 46.

Članice AAI@EduHr prihvaćaju odredbe vezane uz europsku eduroam uslugu danom objave istih na Web adresi http://www.eduroam.hr/.

Članica može u roku od 30 dana od dana objave odredbi iz stavka 1 ovoga članka pisanim putem zatražiti da ne sudjeluje u europskoj usluzi eduroam. U suprotnom smatrat će se da je te odredbe prihvatila.

Ur.broj: 04-7412/007-08

Ravnatelj Srca

mr.sc. Zoran Bekić

PRAVILNIK O USTROJU
Autentikacijske i autorizacijske infrastrukture
znanosti i visokog obrazovanja u Republici Hrvatskoj -
AAI@EduHr