Sveučilište u Zagrebu
Sveučilišni računski centar

Hrvatska akademska i istraživačka mreža

Projekt uspostave
autentikacijske i autorizacijske infrastrukture (AAI)
u sustavu znanosti i visokog obrazovanja

PRAVILA INFORMACIJSKOG ODRŽAVANJA IMENIKA U SUSTAVU AAI@EDUHR

(proizvod AAI.6.1.)

- prijedlog (ver.1.0) -

Zagreb, travanj 2005.

http://www.srce.hr/aai/

Projekt AAI@EduHr

Oznaka proizvoda AAI.6.1

Naziv dokumenta: Pravila informacijskog održavanja imenika u sustavu AAI@EduHr

Verzija i status: ver.1.0 / travanj 2005. / prijedlog

Naziv datoteke: aai@EduHr.6.1.-ver1.0.doc

URL adresa dokumenta: http://www.aaiedu.hr/docs/aai@EduHr.6.1.-ver1.0.pdf

Dokument priredio: Albert Novak

U izradi sudjelovali: Miroslav Milinović, Zoran Bekić

Ovaj je dokument rezultat rada na projektu *Uspostava autentikacijske i autorizacijske infrastrukture (AAI) u sustavu znanosti i visokog obrazovanja – faza A* čije je izvođenje Ministarstvo znanosti, obrazovanja i športa ugovorilo sa Sveučilišnim računskim centrom Sveučilišta u Zagrebu i Hrvatskom akademskom i istraživačkom mrežom – CARNet.

SADRŽAJ

1. Uvod 5
2. AA infrastruktura 5
3. hrEdu shema 6
3.1.Obavezni atributi 6
3.2.Opcionalni atributi 7
4.Politika informacijskog održavanja 7
4.1.Opća pravila 7
4.2.Obaveze održavatelja AAI@EduHr sustava 7
4.3.Prava održavatelja AAI@EduHr sustava 8
4.4.Obveze matične ustanove 8
4.5.Prava matične ustanove 8
4.6.Obaveze vlasnika resursa 9
4.7.Prava vlasnika resursa 9
4.8.Obaveze korisnika 9
4.9.Prava korisnika 9
5.Reference 10

1. Uvod

Važnost autentikacijske i autorizacijske infrastrukture (dalje u tekstu: AAI) proizlaze iz činjenice da je sve većem broju različitih elektroničkih ali i stvarnih, fizičkih resursa i prava moguće ali i potrebno pristupiti, odnosno odobriti pristup elektroničkim putem, najčešće putem Interneta. Pri tome je potrebno osigurati da pristup i/ili realizaciju prava ostvare samo ovlaštene osobe, odnosno osobe koje stvarno imaju pravo uporabe nekog resursa. Ubrzano dolazi vrijeme kada pristup mnogim vitalnim resursima uopće neće biti moguć bez AAI.

Temelj svake AAI jest jasno definiran, pouzdan i efikasan sustav za upravljanje elektroničkim identitetima. Elektronički identitet određen je korisničkom oznakom (hrEduPersonUniqueID atribut hrEduPerson sheme) pri čemu se korisnik jednoznačno povezuje s elektorničkim identitetom znanjem zaporke to jest posjedovanjem privatnog ključa certifikata. Sukladno prijedlogu razvoja AAI akademske i istraživačke zajednice [2], AAI znanosti i visokog obrazovanja u Republici Hrvatskoj (dalje u tekstu: AAI@EduHr) temelji se na distribuiranom sustavu imenika utemeljenih na LDAP tehnologiji.

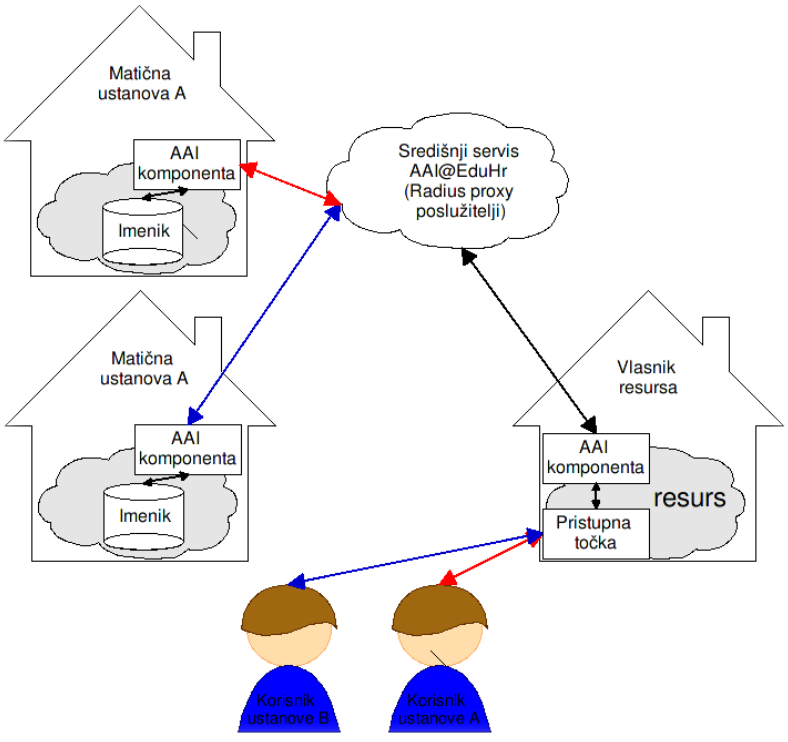
Da bi distribuirani sustav imenika mogao funkcionirati definirana je odgovarajuća jedinstvena zajednička imenička shema [2], odnosno precizan popis atributa s jasnim opisom, semantikom i sintaksom. Imenička shema pri tome predstavlja skup atributa koji su potrebni da bi većina aplikacija koja se oslanja na sustav AAI@EduHr mogla vršiti autentikaciju i autorizaciju.

U ovom dokumentu definiraju se pravila informacijskog održavanja imenika u sustavu AAI@EduHr kojih se moraju pridržavati vlasnici svakog imenika koji želi ući u sustav AAI@EduHr, kao i vlasnici resursa koji žele koristiti sustav u procesu autentikacije i autorizacije.

U ovom dokumentu u točki 2. ukratko je opisana AA infrastruktura s pojedinim subjektima, točka 3. daje kratak osvrt na hrEdu sheme, to jest uporabu obaveznih i opcionalnih atributa, dok točka 4. donosi prava i obaveze svih subjekata AAI@EduHr sustava.

2. AA infrastruktura

Funkcionalna shema sustava AAI@EduHr prikazana je na slici 1.



Slika 1.

Uočimo da u prikazanoj infrastrukturi postoje četiri temeljna subjekta za čije ponašanje je potrebno utvrditi prava i obveze kojih se trebaju pridržavati radi uspješnog rada sustava. To su:

- održavatelj AAI@EduHr sustava;
- matična ustanova;
- vlasnik resursa;
- korisnik.

Održavatelj AAI@EduHr sustava je ovlaštena ustanova koja je odgovorna za: održavanje i unaprjeđivanje cjelokupnog AAI@EduHr sustava, održavanje popisa matičnih ustanova, održavanje popisa vlasnika resursa, održavanje i unaprjeđivanje imeničke hrEdu sheme, to jest provođenje svih onih radnji koje su potrebne da bi distribuirani AAI@EduHr sustav funkcionirao u skladu propisanim pravilima i tehničkim specifikacijama.

Matična ustanova je vlasnik pojedinog imenika u AAI@EduHr i odgovorna je za njegov sadržaj. Matična ustanova imenuje odgovorne osobe za održavanje imenika i provodi registraciju korisnika koji se upisuju u imenik. Matična ustanova i imenovane odgovorne osobe, odgovaraju za točnost podataka o korisnicima koji su uneseni u imenik. Pri tome u imeniku o svakom korisniku mora postojati barem obavezni set atributa propisan hrEdu imeničkom shemom. Sam obavezni set atributa matična ustanova može proširiti i opcionalnim atributima, tako da neke opcionalne atribute za svoje korisnike učini obaveznima, ali pri tome mora izdati odgovarajući pravilnik.

Vlasnik resursa je fizička ili pravna osoba koja posjeduje određeni resurs[1] koji želi ponuditi korisnicima, uz autentikaciju uporabom AAI@EduHr sustava. Vlasnik resursa sam određuje tko i na koji način može koristiti njegove resurse (dakle sam autorizira korisnike ua uporabu resursa) i pri tome koristi AAI@EduHr sustav za autentikaciju korisnika, to jest pojedine atribute iz imenika koji opisuju korisnika u postupku njegove autorizacije za uporabu resursa. Ovdje je važno uviditi da isključivo pravo o načinu korištenja resursa određuje njegov vlasnik i to na temelju postojećih atributa[2] hrEdu imeničke sheme.

Korisnik je osoba registrirana pri njegovoj matičnoj ustanovi, koja uz uporabu AAI@EduHr sustava pristupa nekom resursu, pri čemu AAI@EduHr sustav osigurava autentikacijske i autorizacijske mehanizme i atribute. Korisnik ima mogućnost samostalnog upravljanja određenim atributima u skladu sa pravilima koja propisuje održavatelj AAI@EduHr sustava i njegova matična ustanova.

3. hrEdu sheme

hrEdu imeničke sheme[2] su:

- hrEduPerson shema za podatke o osobama
- hrEduOrg shema za podatke o ustanovama,

Atributi predloženi u hrEdu shemama [2] 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.

---

[1] Resurs je objekt kojem korisnik želi pristupiti; može biti računalna mreža, sustav, Web sjedište, aplikacija, ...

[2] Vlasnik resursa može koristiti i dodatne atribute kojima kontrolira pristup resursu. Npr. ukoliko vlasnik resursa nudi pristup mrežnom printeru studentima čija je upotreba ograničena na određeni broj ispisanih stranica, vlasnik resursa može unutar svog sustava za kontrolu ispisa na mrežni printer dodati atribut koji sadrži podatak o broju ispisanih stranica svakog korisnika printera i na osnovu njega ograničavati daljnje korištenje resursa. Pri tome se za pristup samom printeru koriste atributi korisnika putem AAI@EduHr sustava dok se lokalni atribut o trenutnom broju ispisanih stranica koristi za ograničavanje broja ispisanih stranica.

Atributi predloženi u hrEdu shemi podložni su promjenama i svaki sudionik u AAI@EduHr sustavu ima pravo predlagati promjenu postojećih atributa ili dodavanje novih održavatelju AAI@EduHr sustava putem Registra shema dostupnog na adresi http://schema.aaiedu.hr/. O promjenama atributa odlučuje održavatelj AAI@EduHr sustava.

3.1. Obavezni atributi

Svaki zapis u LDAP imeniku mora imati minimalno set obaveznih atributa navedenih u hrEdu shemi da bi mogao egzistirati unutar AAI@EduHr sustava. Matična ustanova koja kreira elektroničke identitete unutar svog imenika dužna je osigurati da unutar imenika bude popunjen barem minimalni set atributa.

Resursi koji koriste AAI@EduHr mogu uvijek koristiti obavezne atribute u procesu autentikacije i autorizacije jer svaka matična ustanova mora osigurati da je taj minimalan set atributa unešen i ažuran.

Pošto matična ustanova mora osigurati da svaki zapis LDAP imenika ima barem minimalan set obaveznih atributa, preporuka je do održavanje ažurnosti tih atributa bude u isključivoj nadležnosti matične ustanove.

3.2. Opcionalni atributi

hrEdu shemom je predviđen i određen broj opcionalnih atributa. Prepušteno je, na nivou AAI@EduHr sustava, matičnim ustanovama da odrede kako će upravljati pojedinim opcionalnim atributima, to jest koje će od opcionalnih atributa koristiti.

Pri tome valja naglasiti da pojedini opcionalni atributi mogu biti ključni za korištenje pojedinih resursa te ukoliko nisu uneseni neće biti moguće pristupiti to jest koristiti određene resurse.

Preporuka je da se o ažurnosti opcionalnih atributa brine fizička osoba na koju se odnosi elektronički identitet ukoliko matična ustanova i održavatelj AAI@EduHr sustava ne odredi drugačije.

4. Politika informacijskog održavanja

Ova politika uređuje prava i obveze informacijskog održavanja AAI@EduHR sustava, to jest pravila i procedure kojih se mora pridržavati prilikom svih interakcija između vlasnika resursa, matične ustanove i korisnika resursa koji se odnose na autentikaciju i autorizaciju.

S obzirom da od stanja podataka u sustavu distribuiranih imenika unutar AAI@EduHr ovisi pravo i mogućnost korisnika da pristupaju mnogim elektroničkim, virtualnim ali i stvarnim fizičkim resursima, održavanje urednog informacijskog stanja imenika podrazumjeva odgovoran odnos svih subjekata u AAI@EduHr prema pravilima, pravima i obavezama propisanim u nastavku ovog poglavlja.

4.1. Opća pravila

4.1.1. Svi sudionici AAI@EduHr sustava dužni su održavati AAI programsku podršku u skladu sa preporukama održavatelja AAI@EduHr sustava.

4.1.2. S osobnim podacima, to jest zbirkama osobnih podataka, treba se ponašati u skladu sa važećim zakonima Republike Hrvatske.

4.1.3. U procesu autentikacije i autorizacije treba korisiti minimalni set atributa koji je nužan za autentikaciju i autorizaciju pristupa pojedinom resursu.

4.1.4. Svaka fizička osoba o kojoj se prikupljaju osobni podaci potrebni za rad AAI@EduHr sustava, na vlastiti zahtjev, mora biti informirana o osobnim podacima koji pojedini resursi prikupljaju o njoj.

4.2. Obaveze održavatelja AAI@EduHr sustava

4.2.1. Održavatelj AAI@EduHr dužan je održavati službeni središnji web sustava http://www.aaiedu.hr.

4.2.2. Održavatelj AAI@EduHr sustava dužni su održavati popis matičnih organizacija na službenom središnjem webu AAI@EduHr sustava.

4.2.3. Održavatelji AAI@EduHr sustava dužni su održavati popis vlasnika resursa koji koriste AAI@EduHr sustav za autentikaciju i autorizaciju zajedno s popisom atributa koji oni prikupljaju na službenom središnjem webu AAI@EduHr sustava.

4.2.4. Održavatelji AAI@EduHr sustava dužni su održavati i unaprjeđivati AAI@EduHr sustav.

4.2.5. Održavatelj AAI@EDuHr sustava dužan je prikupljati primjedbe i prijedloge proširenja na postojeće sheme i provoditi postupke izmjene istih.

4.3. Prava održavatelja AAI@EduHr sustava

4.3.1. Održavatelji AAI@EduHr sustava imaju pravo isključiti iz AAI@EduHr sustava one vlasnike resursa, kao i matične ustanove koje ne poštuju ova i druga pravila za održavanje i upotrebu AAI@EduHr sustava.

4.4. Obveze matične ustanove

4.4.1. Matične ustanove dužne su imenovati ovlaštene osobe zadužene za održavanje imenika. Preporuka je da ovlaštene osobe čine 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.

4.4.2. Matične ustanove dužne su imenovati kontakt osobu zaduženu za komunikaciju s održavateljima AAI@EduHr sustava, te o tome izvjesiti održavatelja AAI@EduHr sustava.

4.4.3. Prije prikupljanja osobnih podataka ovlaštene osobe matičnih ustanova dužne su informirati korisnika kojeg registriraju o svrsi obrade kojoj su podaci namijenjeni, kategorijama korisnika podataka kao i mogućim posljedicama uskrate podataka.

4.4.4. 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 (zaporke, pin i sl.).

4.4.5. Uprave i ovlaštene osobe matične ustanove dužne su se brinuti o ažurnosti podataka koji su u nadležnosti matične ustanove, pri čemu se prvenstveno misli na povezanost vlasnika elektroničkog identiteta s matičnom ustanovom, to jest sve obvezne atribute. Neaužurnim podacima otvara se mogućnost zlouporabe elektroničkog identiteta prilikom pristupanja resursima.

4.4.6. Matična ustanova je dužna ukloniti elektronički identitet iz imenika svih onih korisnika s kojima se ne može uspostaviti temeljna pripadnost ustanovi kako je to definirano šifrarnikom u hrEduPearson shemi.

4.4.7. 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, to jest resursima koji se nalaze na popisu održavatelja AAI@EduHr sustava.

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

4.4.9. Na pismeni zahtjev korisnika matična ustanova je dužna izbrisati njegov elektronički identitet iz imenika pri čemu je matična ustanova obavezna upozoriti korisnika na posljedice brisanja elektroničkog identiteta iz AAI@EduHr sustava.

4.5. Prava matične ustanove

4.5.1. Svaka matična ustanova može samostalno odrediti set obaveznih atributa podataka koji se prikupljaju ali pritom mora poštivati minimum koji zahtijeva AAI@EduHr shema [3].

4.5.2. Matična ustanova ima pravo proširivati set atributa eduHR sheme za svoju lokalnu upotrebu.

4.6. Obaveze vlasnika resursa

4.6.1. Vlasnik resursa dužan se registrirati kod održavatelja AAI@EduHR sustava i prijaviti mu atribute koje želi koristiti prilikom kontrole pristupa resursima koje daje na upotrebu korisnicima.

4.6.2. Vlasnik resursa prilikom autentikacije i autorizacije korištenjem AAI@EduHr sustava mora koristiti minimalan set atributa nužan za proces autentikacije i autorizacije.

4.6.3. Vlasnik resursa koji koristi AAI@EduHr sustav u procesu autentikacije i autorizacije dužan je koristiti dostupne sigurnosne mehanizme kako prilikom transporta tako i prilikom pohrane atributa koje koristi u procesu autentikacije i autorizacije.

4.6.4. Vlasnik resursa nesmije pohranjivati korištene atribute u procesu autentikacije i autorizacije osim za potrebe kreiranja logova pri čemu mora u sigurnosnoj politici imati navedenu svrhu kreiranja i vrijeme čuvanja loga. U logu se smije pohranjivati samo minimalni set atributa.

4.6.5. Vlasnik resursa, korištene atribute, smije koristiti samo u svrhu autentikacije i autorizacije prilikom pristupa resursima koje daje na uporabu korisnicima.

4.7. Prava vlasnika resursa

4.7.1. Vlasnik resursa samostalno određuje tko i na koji način, to jest putem kojih atributa, može pristupati resursu koji on daje na upotrebu korisnicima AAI@EduHr sustava.

4.8. Obaveze korisnika

4.8.1. Korisnik je odgovoran za točnost i ažurnost podataka koje ustanova stavi u njegovu nadležnost.

4.8.2. Korisnik je dužan čuvati povjerljivost podataka kojima dokazuje svoj identitet (zaporka, pin i sl.), te ne ustupati iste za pristup datim mu resursima drugim osobama.

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

4.8.4. U slučaju promjene osobnih podataka u odnosu na one unesene u imeniku, kao i u slučaju uočavanja netočnih podatka čiji unos je u nadležnosti imenovane odgovorne osobe na matičnoj ustanovi, korisnik je obavezan izvjestiti odgovornu osobu na matičnoj ustanovi.

4.9. Prava korisnika

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

4.9.2. Korisnik ima pravo od održavatelja AAI@EduHr dobiti popis vlasnika resursa koji koriste podatke iz imenika za pristup resursima.

4.9.3. Korisnik ima pravo dobiti od vlasnika resursa popis atributa koje koristi prilikom autentikacije i autorizacije korisnika.

4.9.4. Korisnik ima pravo od matične ustanove pismeno zatražiti da se izbriše njegov elektronički identitet iz imenika što je ova dužna i izvršiti.

5. Reference

[1] Prijedlog razvoja autentikacijske i autorizacijske infrastrukture (AAI) akademske i istraživačke zajednice u Republici Hrvatskoj (ver.1.2.)

[2] Definicija hrEdu imeničkih shema (ver.1.1.)