Sustav provjere usklađenosti (certificiranja) matičnih ustanova i davatelja usluga s normama Autentikacijske i autorizacijske infrastrukture znanosti i visokog obrazovanja u Republici Hrvatskoj - AAI@EduHr

SADRŽAJ

verzija 1.2, lipanj 2010

1. UVOD

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.

Kako bi AAI@EduHr sigurno i pouzdano ispunila svoju zadaću nužno je da su svi njeni elementi usklađeni s odgovarajućim normama kako u organizacijskom tako i u informacijskom i tehničkom smislu.

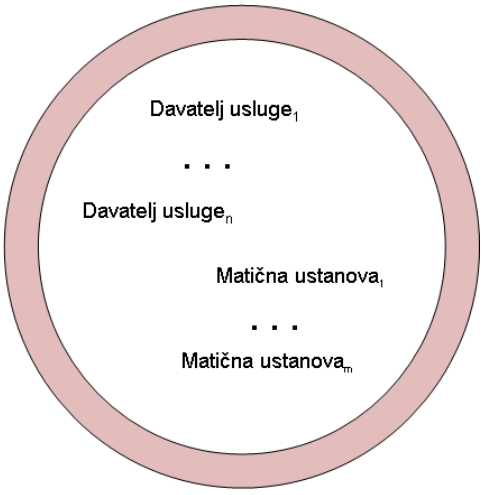
Temeljne norme sustava AAI@EduHr definirane su **Pravilnikom o ustroju Autentikacijske i autorizacijske infrastrukture znanosti i visokog obrazovanja u Republici Hrvatskoj - AAI@EduHr**. Detalje organizacijskih, informacijskih i tehničkih normi, sukladno Pravilniku, propisuje Koordinator AAI@EduHr – Srce.

Ovim dokumentom definira se **Sustav provjere usklađenosti (certificiranja) matičnih ustanova i davatelja usluga s normama AAI@EduHr** (dalje: Sustav provjere) te se, ovisno o ulozi koju pojedini subjekt obnaša u sustavu AAI@EduHr, određuju parametri i način na koji se provodi provjera usklađenosti.

2. USTROJ I NORME AAI@EDUHR

Organizacijski, informacijski i tehnički ustroj sustava AAI@EduHr definiran je odgovarajućim Pravilnikom o ustroju. Pravilnik definira osnove norme te određuje da je za njihovo provođenje te izradu i koordinaciju primjene odgovarajućih pravila i naputaka zadužen Koordinator sustava AAI@EduHr.

Pravilnikom o ustroju, sustav AAI@EduHr definiran je kao federacija ustanova članica koje mogu obnašati ulogu matične ustanove i/ili davatelja usluge. U tom smislu na sustav AAI@EduHr može se gledati kao na krug povjerenja u kojem svi subjekti s povjerenjem u kvalitetu i pouzdanost prihvaćaju elektroničke identitete izdane od strane matičnih ustanova (vidi sliku 1.)



Slika 1. – krug povjerenja

Kako bi se jednom uspostavljeno povjerenje očuvalo, neophodno je da se svi subjekti sustava pridržavaju odgovarajućih normi. Stoga je nužno ustrojiti sustav kojim se provjerava stupanj usklađenosti pojedinog subjekta s normama sustava. Samu je provjeru potrebno provoditi ne samo prilikom uključivanja novih subjekata u sustav, nego i redovito kako bi se osigurala trajna pouzdanost cjelokupnog sustava.

3. SUSTAV PROVJERE

3.1. O sustavu

Sustav provjere ustrojen je tako da omogući provjeru usklađenosti sa sve 3 vrste normi u AAI@EduHr:

- organizacijskim,
- informacijskim,
- tehničkim.

Provjeru provodi:

- Koordinator AAI@EduHr
    - automatizirano, uporabom odgovarajuće opreme i programskih alata,
    - pojedinačnim, neposrednim uvidom u aktivnosti subjekta,
    - uvidom u službenu dokumentaciju sustava AAI@EduHr;
- subjekt (ustanova članica ili partner federacije)
    - popunjavanjem elektroničkih obrazaca za samoprovjeru,
    - pokretanjem odgovarajućeg programa prema uputama Koordinatora.

Temeljem provedene provjere Koordinator donosi odluku o razini usklađenosti. Obavijest o donešenoj odluci, odnosno rezultatima provjere Koordinator pisanim putem dostavlja čelniku subjekta te objavljuje putem javno dostupnog web sjedišta na adresi www.aaiedu.hr.

Svi subjekti (ustanove članice i partneri) dužni su sudjelovati u procesu provjere.

U sustavu AAI@EduHr utvrđuju se 3 razine usklađenosti s normama AAI@EduHr:

- **razina 1: dovoljna usklađenost**
- **razina 2: dobra usklađenost**
- **razina 3: izvrsna usklađenost.**

Subjekt ima razinu usklađenosti 1 ukoliko pri provjeri zadovolji sve obavezne norme.

Subjekt ima razinu usklađenosti 2 ukoliko pri provjeri zadovolji sve obavezne i barem 50% preporučenih normi.

Subjekt ima razinu usklađenosti 3 ukoliko pri provjeri zadovolji sve obavezne i preporučene norme.

Provjera usklađenosti obavlja se jednom godišnje za sve subjekte sustava, a iznimno na zahtjev nekog subjekta, korisnika ili po odluci Koordinatora i češće. Koordinator ima pravo, neposrednim uvidom u stanje, provjeriti rezultate koje je subjekt ostvario samoprovjerom.

Način obavljanja provjere ovisi o ulozi koju subjekt obnaša (matična ustanova ili davatelj usluge).

Subjektima koji ne dosegnu razinu 1 ili ne sudjeluju u procesu provjere ostavlja se rok od 2 mjeseca da to učine. Nakon toga roka Koordinator pisanim putem izvješćuje čelnika subjekta o nedovoljnoj usklađenosti sa sustavom AAI@EduHr uz dodatni rok od 1 mjeseca za postizanje razine 1. Ne postigne li subjekt razinu 1 i nakon dodatnog roka, Koordinator podnosi Savjetu

AAI@EduHr prijedlog za privremeno isključenje subjekta iz sustava AAI@EduHr. Privremeno isključeni subjekt može biti ponovno uključen u sustav AAI@EduHr tek kad dostigne razinu 1.

3.2. Provjera matičnih ustanova

Temeljna prava i obveze matičnih ustanova definirana su točkom 3.6. Pravilnika u ustroju AAI@EduHr.

Prilikom provjere matičnih ustanova posebni je naglasak stavljen na informacijsku potpunost i ažurnost imenika te procedure kojima se dodjeljuju i održavaju elektronički identiteti. U tehničkom dijelu zahtjeva se pouzdanost AAI@EduHr komponente na matičnoj ustanovi (LDAP imenik, RADIUS poslužitelj, AOSI web servis).

Norma	Opis	Status (razina)	Način provjere
1. Formalno članstvo	Potpisan, ovjeren i odobren odgovarajući zahtjev	obavezno	Koordinator – pisana arhiva
2. Imenovani predstavnici	Imenovane kontakt osobe i predstavnik u Vijeću AAI@EduHr	obavezno	Koordinator – pisana arhiva
3. Prijava AZOP-u	LDAP imenik prijavljen AZOP-u	preporučeno	Ustanova – samoprovjerom
4. Procedura za informacijsko održavanje imenika	Utvrđena procedura za informacijsko održavanje imenika	obavezno preporučeno: procedura je javno dostupna	Ustanova – samoprovjerom
5. Informiranje korisnika	Korisnici su informirani o svojim pravima i obavezama prilikom preuzimanja e-identiteta	obavezno	Ustanova – samoprovjerom
6. Postojanje evidencije	Matična ustanova vodi evidenciju o dodijeljenim e-identitetima	obavezno	Ustanova – samoprovjerom
7. Kontakt podaci za korisnike	Podaci o ovlaštenim osobama te kontakt podaci za korisnike objavljeni su u registru matičnih ustanova i na www.aaiedu.hr	obavezno	Koordinator – uvid u podatke u registru matičnih ustanova
8. Obuhvaćenost e-identitetima	Svi zaposlenici i studenti posjeduju e-identitete	preporučeno	Ustanova – samoprovjerom
9. Provjera identiteta osobe pri dodjeli e-identiteta	Dodjela e-identiteta obavlja se na temelju dokumenta sa slikom ili kroz proces zapošljavanja/upisa	obavezno	Ustanova – samoprovjerom

Norma	Opis	Status (razina)	Način provjere
10. Postupak uručenja e-identiteta	Podaci o e-identitetu se uručuju osobno ili pisanim putem (ne telefonom ili e-mailom). Odnosi se i na promjenu lozinke.	obavezno	Ustanova – samoprovjerom
11. Brisanje e-identiteta	E-identiteti osoba koje su prestale biti povezane s ustanovom se pravodobno i redovito brišu (sukladno utvrđenoj proceduri)	obavezno	Ustanova – samoprovjerom
12. Informacijska kvaliteta imenika: istekli e-identiteti	Broj e-identiteta koji su označeni kao istekli prije više od 3 mjeseca (u to se broje i studentski e-identiteti bez podatka o isteku)	preporučeno: broj je 0 obavezno: broj je manji od 1% od ukupnog broja e-identiteta u imeniku	Koordinator i ustanova – program za analizu sadržaja imenika
13. Informacijska kvaliteta imenika: elektroničke adrese	Broj e-identiteta koji nemaju ispravan podatak o e-mail adresi	preporučeno: broj je 0 obavezno: broj je manji od 1% od ukupnog broja e-identiteta u imeniku	Koordinator i ustanova – program za analizu sadržaja imenika
14. Informacijska kvaliteta imenika: OIB	Uz svaki je e-identitet zabilježen odgovarajući OIB	preporučeno	Koordinator i ustanova – program za analizu sadržaja imenika
15. Informacijska kvaliteta imenika: brojčani identifikator	Vrijednost atributa *brojčani identifikator osobe* je jedinstvena na nivou ustanove	obavezno	Koordinator i ustanova – program za analizu sadržaja imenika
16. Informacijska kvaliteta imenika: podaci o ustanovi (hrOrg atributi)	Potpunost i ispravnost podataka o ustanovi zapisanih u imeniku	obavezno	Koordinator i ustanova – program za analizu sadržaja imenika
17. Nadzor AAI@EduHr komponente	Koordinatoru je omogućen nadzor rada LDAP, RADIUS i AOSI-WS poslužitelja	obavezno	Koordinator – sustav nadzora

Norma	Opis	Status (razina)	Način provjere
18. Programska podrška: LDAP	Instalirana i ispravno konfigurirana posljednja inačica LDAP programskog paketa iz distribucije AAI@EduHr ili drugog odgovarajućeg programa	obavezno: inačica koju Koordinator označi kritičnom ili novija preporučeno: najnovija dostupna inačica	Koordinator – sustav nadzora
19. Programska podrška: RADIUS	Instalirana i ispravno konfigurirana posljednja inačica RADIUS programskog paketa iz distribucije AAI@EduHr ili drugog odgovarajućeg programa	obavezno: inačica koju Koordinator označi kritičnom ili novija preporučeno: najnovija dostupna inačica	Koordinator – sustav nadzora
20. Programska podrška: AOSI-WS	Instalirana i ispravno konfigurirana posljednja inačica odgovarajućeg programskog paketa iz distribucije AAI@EduHr	obavezno: inačica koju Koordinator označi kritičnom ili novija preporučeno: najnovija dostupna inačica	Koordinator – sustav nadzora
21. Sekundarni servisi	U produkciji su sekundarni LDAP, RADIUS i AOSI-WS	preporučeno	Koordinator – sustav nadzora
22. Postojanje uputa i web sučelja za vlasnike e-identiteta	AOSI-web sučelje, ISVU web sučelje ili vlastito rješenje	obavezno	Koordinator – sustav nadzora
23. certifikat RADIUS poslužitelja	Vršni (root) certifikat koji je korišten pri generiranju certifikata za RADIUS poslužitelj ustanove objavljen u elektroničkom obliku te dostupan korisnicima, a certifikat RADIUS poslužitelja ustanove ispravan	preporučeno	Ustanova – samoprovjerom; Koordinator – sustav nadzora

3.3. Provjera davatelja usluga

Temeljna prava i obveze davatelja usluga definirana su točkom 3.7. Pravilnika u ustroju AAI@EduHr.

Prilikom provjere davatelja usluga posebni je naglasak stavljen na poštivanje tehničkih normi sustava AAI@EduHr.

Ukoliko davatelj istodobno nudi više usluga, provjerava se svaka od njih, ovisno o konkretnoj normi koju je potrebno ispuniti.

Norma	Opis	Status (razina)	Način provjere
1. Formalno članstvo	Potpisan, ovjeren i odobren odgovarajući zahtjev	obavezno	Koordinator – pisana arhiva
2. Imenovani predstavnici	Imenovane kontakt osobe i predstavnici u Vijeću AAI@EduHr	obavezno: imenovanje kontakt osobe preporučeno (za partnere): imenovanje predstavnika u Vijeću AAI@EduHr	Koordinator – pisana arhiva
3. Korišteni protokoli	Sukladno preporuci Koordinatora: RADIUS za pristup mreži i računalnim resursima; HTTP/SOAP za Web resurse	obavezno	Koordinator – registar resursa
4. Korišteni središnji servisi za Web resurse	SSO/login ili FWS	obavezno preporučeno: SSO/login	Koordinator – registar resursa
5. Zapis u registru resursa	Točnost i potpunost podataka u registru	obavezno	Koordinator – registar resursa i sustav nadzora
6. Način uporabe središnjih servisa AAI@EduHr	Koristi središnje servise AAI@EduHr sukladno uputama Koordinatora	obavezno	Koordinator – nadzor rada središnjih servisa