Preporuke za upravljanje elektroničkim identitetima u sustavu AAI@EduHr

Pravila vezana uz upravljanje elektroničkim identitetima

Pravilnik o ustroju Autentikacijske i autorizacijske infrastrukture znanosti i visokog obrazovanja u Republici Hrvatskoj - AAI@EduHr u članku 29. definira obaveze matičnih ustanova na sljedeći način:

- 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;
- 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;

Provjere (certificiranje matičnih ustanova) koje provodi Srce

Postupke upravljanja elektroničkim identitetima provjeravamo jednom godišnje u postupku certificiranja matičnih ustanova u AAI@EduHr sustavu. Posebno bismo ovdje izdvojili norme koje se odnose na upravljanje elektroničkim identitetima:

- **Je li utvrđena procedura za informacijsko održavanje imenika?**
  Svaka bi ustanova trebala imati proceduru kojom se propisuje tko i pod kojim uvjetima ima pravo na elektronički identitet unutar imenika ustanove, te kako to pravo gubi. Primjer procedure Metalurškog fakulteta Sveučilišta u Zagrebu možete vidjeti u Proceduri za informacijsko održavanje imenika Metalurškog fakulteta.

- **Je li procedura za informacijsko održavanje imenika javno dostupna?**
  U svrhu upoznavanja korisnika, a i ostalih subjekata u sustavu s procedurom za informacijsko održavanje imenika, ta bi procedura trebala biti javno dostupna.

- **Jesu li korisnici informirani o svojim pravima i obavezama prilikom preuzimanja e-identiteta?**
  Sukladno Pravilniku, korisnici bi prilikom preuzimanja svog elektroničkog identiteta trebali biti informirani o svojim pravima i obvezama:

  - 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.
  - 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 je dužan pridržavati se pravila pojedine usluge kojom pristupa svojim elektroničkim identitetom.

  AOSI web sučelje ima mogućnost ispisa prilagođenog izvještaja o otvorenom elektroničkom identitetu. Naša je preporuka da, sukladno proceduri za informacijsko održavanje imenika ustanove, uredite taj izvještaj, dopunite ga pravima i obavezama korisnika (i ostalim potrebnim detaljima vezanim uz vašu ustanovu), te svakom korisniku po otvaranju elektroničkog identiteta uručite takav izvještaj.

- **Vodi li matična ustanova evidenciju o dodijeljenim e-identitetima?**
  Matična je ustanova dužna voditi evidenciju o svim izdanim elektroničkim identitetima.

- **Obavlja li se dodjela e-identiteta se na temelju dokumenta sa slikom ili kroz proces zapošljavanja/upisa?**
  Naša je preporuka da posao administracije elektroničkih identiteta obavlja kadrovska služba / studentska referada. Prilikom dodjele elektroničkog identiteta OBAVEZNA je provjera identiteta korisnika.

- **Uručuju li se podaci o e-identitetu osobno ili pisanim putem (ne telefonom ili e-mailom)? Odnosi se i na promjenu lozinke.**
  U svrhu smanjenja mogućnosti kompromitiranja elektroničkog identiteta, podaci o elektroničkom identitetu trebali bi se korisnicima uručivati osobno uz provjeru identiteta ili poštom. Ustanova je dužna osigurati da se podaci o elektroničkom identitetu korisniku isporučuju na siguran i zaštićen način. E-mail nije siguran medij pa nije dozvoljeno podatke o elektroničkom identitetu slati e-mailom. **ZABRANJENO** je dodjeljivati elektroničke identitete javnom objavom (npr. na oglasnoj ploči, webu i sl.), dodjeljivati lozinke javno objavljenim algoritmom koji može ugroziti sigurnost elektroničkih identiteta, slati podatke o elektroničkom identitetu posredstvom trećih osoba na nezaštićen način i sl.

- **E-identiteti osoba koje su prestale biti povezane s ustanovom se pravodobno i redovito se brišu (sukladno utvrđenoj proceduri).**
  Kako bi se onemogućilo da osoba koja više nema pravo na elektronički identitet pristupa uslugama dostupnima u AAI@EduHr sustavu, takve elektroničke identitete treba redovito brisati (a u skladu s procedurom za informacijsko održavanje imenika).

- **Je li 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) manji od 1% ukupnog broja korisnika u LDAP imeniku?**
  Jedan od pokazatelja (ne)ažurnosti imenika je ima li u imeniku isteklih elektroničkih identiteta. Naša je preporuka svima čija je povezanost s ustanovom vremenski ograničena (npr. studentima dok traju studentska prava), upisati datum isteka povezanosti s ustanovom. Osobe koje su trajno povezane s ustanovom (npr. djelatnici zaposleni na neodređeno vrijeme) ne trebaju imati postavljen datum isteka. Administrator imenika dužan je informacije u imeniku držati ažurnima, pa tako i ažurirati datum isteka temeljne povezanosti s ustanovom sukladno sa statusom korisnika.

Iz prakse

U praksi nalazimo i dobrih i loših primjera vezanih uz upravljanje elektroničkim identitetima.

Dobri primjeri:

- Procedura za informacijsko održavanje imenika Metalurškog fakulteta Sveučilišta u Zagrebu.

Loši primjeri, postupci kojima se narušava sigurnost i privatnost korisnika, a time i povjerenje u cjelokupni sustav AAI@EduHr. Ovi su postupci u suprotnosti s Pravilnikom o ustroju AAI@EduHr:

- Slanje elektroničkog identiteta (i zaporke koja je njegov dio) elektroničkom poštom;
- Objava algoritma kojim je inicijalno postavljena zaporka elektroničkim identitetima (na način da se zaporka sastoji od podataka dostupnih trećim osobama);
- Uručivanje podataka (posebno zaporke) o elektroničkom identitetu bez provjere identiteta osobe kojoj se uručuju;