

**Provjera usklađenosti (certificiranje) usluga s normama
Autentikacijske i autorizacijske infrastrukture znanosti i
visokog obrazovanja u Republici Hrvatskoj - AAI@EduHr
za 2019. godinu**



SADRŽAJ

| | |
|--|----------|
| 1. SUSTAV PROVJERE USKLAĐENOSTI (CERTIFICIRANJA) USLUGA | 2 |
| 2. POPIS NORMI ZA 2019. GODINU | 3 |

verzija 1.0 svibanj 2019.

1. SUSTAV PROVJERE USKLAĐENOSTI (CERTIFICIRANJA) USLUGA

Sustav certificiranja definiran je dokumentom koji je javno dostupan na adresi https://www.aaiedu.hr/sites/default/files/content_files/docs/aaieduhr-idp-certificiranje-2009-v1.2.pdf.

Temeljna prava i obveze davatelja usluga definirani su točkom 3.7. Pravilnika u ustroju AAI@EduHr (https://www.aaiedu.hr/sites/default/files/content_files/docs/AAI%40EduHr-pravilnik-ver1.3.1.pdf)

Certificiranje usluga za 2019. godinu provodit će se u vremenu od 3. lipnja do 15. srpnja 2019. O eventualnom dopunskom roku Koordinator AAI@EduHr – Srce će obavijestiti davatelje usluga nakon 15. srpnja 2019.

Sukladno ranije spomenutom dokumentu provjeru provodi Koordinator AAI@EduHr:

- automatizirano, uporabom odgovarajuće opreme i programskih alata
- pojedinačnim, neposrednim uvidom u način rada usluge
- uvidom u službenu dokumentaciju sustava AAI@EduHr i sadržaj registra resursa (<https://registar.aaiedu.hr/>).

Svi davatelji usluga dužni su sudjelovati u procesu provjere. Ukoliko davatelj nudi više usluga, provjerava se svaka od njih.

Certificiranjem će biti obuhvaćene sve usluge koje su u registru označene kao produkcijske. U sustavu AAI@EduHr utvrđene su 3 razine usklađenosti s normama AAI@EduHr:

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

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

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

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

Temeljem provedene provjere Koordinator će utvrditi razinu usklađenosti te objaviti odgovarajuće informacije putem javno dostupnog web sjedišta na adresi <http://www.aaiedu.hr/>. Zbirni izvještaj o provedenom certificiranju Koordinator će dostaviti Savjetu AAI@EduHr i MZO.

Davateljima usluga koje ne dosegnu razinu 1 ostavit će se rok od 2 mjeseca da obave potrebne preinake kako bi usluga dosegla razinu 1. Nakon toga roka Koordinator će pisanim putem izvijestiti čelnika ustanove koja daje uslugu o nedovoljnoj usklađenosti sa sustavom AAI@EduHr uz dodatni rok od 1 mjesec za postizanje razine 1. Ne postigne li usluga razinu 1 i nakon dodatnog roka, Koordinator može privremeno isključiti uslugu iz sustava AAI@EduHr. Privremeno isključena usluga može biti ponovno uključena u sustav AAI@EduHr tek kad dostigne razinu 1.

2. POPIS NORMI ZA 2019. GODINU

| Norma | Opis uvjeta koji se provjerava | Status | Način provjere |
|--|--|-------------|--|
| 1. Formalno članstvo | Je li potpisan, ovjeren i odobren odgovarajući zahtjev za članstvo ili status partnera u sustavu AAI@EduHr? | obavezno | Koordinator (pisana arhiva) |
| 2. Poštivanje Pravilnika o ustroju AAI@EduHr | Odgovorna osoba davatelja usluge je prilikom registracije usluge potvrdila kako će usluga biti pružana sukladno odredbama Pravilnika o ustroju AAI@EduHr (točka 3.7.). | obavezno | Koordinator (registar resursa) |
| 3. Zapis u registru resursa - naziv | U registar resursa upisan je točan, jasan i krajnjem korisniku razumljiv, naziv usluge. | obavezno | Koordinator (registar resursa) |
| 4. Zapis u registru resursa – URL adresa | U registar resursa upisana je točna: - URL adresa usluge (ako se radi o usluzi dostupnoj HTTP(S) protokolom) ili - web stranica s informacijama o usluzi (ako se radi o usluzi koja nije dostupna HTTP(S) protokolom). | obavezno | Koordinator (registar resursa) |
| 5. Zapis u registru resursa – opis | U registar resursa upisan je jasan i točan opis usluge. | obavezno | Koordinator (registar resursa) |
| 6. Zapis u registru resursa – administrator | U registar resursa upisani su točni podaci o administratoru (odgovornoj osobi) usluge. | obavezno | Koordinator (registar resursa) |
| 7. Korišteni protokoli | Za pristup središnjim servisima usluga koristi protokol: - SAML 2.0 ili CAS (ako se radi o usluzi dostupnoj HTTP(S) protokolom) - RADIUS (ako se radi o usluzi koja nije dostupna HTTP(S) protokolom). | obavezno | Koordinator (registar resursa i središnji nadzorni sustav) |
| 8. Poštivanje Opće uredbe o zaštiti osobnih podataka (GDPR) | Prilikom pristupanja usluzi korisnici su obaviješteni o svrsi prikupljanja i načinu obrade njihovih osobnih podataka. Na stranicama usluge objavljena je politika privatnosti. | preporučeno | Koordinator (registar resursa i uvid u uslugu) |

| Norma | Opis uvjeta koji se provjerava | Status | Način provjere |
|--|---|-------------|---|
| Posebne norme za usluge dostupne HTTP(S) protokolom | | | |
| 9. Korištenje HTTPS protokola | Usluga koristi isključivo HTTPS protokol. | preporučeno | Koordinator (registar resursa) |
| 10. Single log-out (SLO) | Usluga ima implementiranu središnju odjavu korisnika (single log-out). | preporučeno | Koordinator (registar resursa) |
| 11. Korištenje certifikata | Usluga koristi certifikat izdan putem CARNetove TCS usluge ili izravno od izdavača evidentiranog u početnim postavkama popularnih | preporučeno | Koordinator (središnji nadzorni sustav) |
| Posebne norme za usluge koje nisu dostupne HTTP(S) protokolom | | | |
| 12. Način rada RADIUS poslužitelja | RADIUS poslužitelj usluge ispravno prosljeđuje upite središnjim poslužiteljima, koristeći EAP protokol. | obavezno | Koordinator (središnji nadzorni sustav) |
| 13. Isporuka atributa | RADIUS poslužitelj usluge ne modificira atribute koje prosljeđuje središnjim poslužiteljima. | obavezno | Koordinator (središnji nadzorni sustav) |
| 14. Isporuka atributa ON | RADIUS poslužitelj usluge ispravno isporučuje RADIUS atribut ON (OperatorName). | obavezno | Koordinator (središnji nadzorni sustav) |