



## Dobili smo ArnesAAI, kaj sledi? We've got ArnesAAI, what next?

### Povzetek

Arnes AAI pridruženim organizacijam poenostavlja upravljanje uporabniških imen in gesel ter njihovim uporabnikom daje možnost uporabe aplikacij, ki so vključene v ArnesAAI (npr. spletne konference VOX), ali katere izmed lastnih aplikacij, ki podpirajo tovrstno prijavo. Organizacije se lahko v Slovensko izobraževalno raziskovalno federacijo ArnesAAI pridružijo na več načinov, prav tako lahko uporabniki, če njihova organizacija ni članica federacije ArnesAAI, vseeno pridobijo uporabniško ime, ki jim nudi omejene funkcionalnosti.

**Ključne besede:** ArnesAAI, ponudnik identitet, ponudnik storitev, enotno uporabniško ime.

### Abstract

ArnesAAI makes it easier for affiliated organisations to manage user names and passwords, and allows users to use applications bundled with ArnesAAI (e.g. Vox webconferences), as well as their own applications that support this type of login. Organisations have various options for joining ArnesAAI, the Slovenian education-research federation, and users can get limited-functionality NetIDs even if their organisation is not a member of the ArnesAAI federation.

**Key words:** ArnesAAI, identity provider, service provider, single sign-on

### Uvod

Vse večja uporaba informacijskih tehnologij v raziskovalno-izobraževalni sferi s seboj prinaša veliko število uporabniških podatkov. Hramba, varovanje in osveževanje podatkov predstavlja za tehnično osebje na organizacijah velik zalogaj. Namesto izdajanja novih uporabniških imen in gesel za različne storitve lahko kot rešitev uvedemo centralizirane in enotno strukturirane zbirke uporabniških podatkov in infrastrukturo, ki bo omogočala sodelovanje med organizacijami. S tem je mogoče končnim uporabnikom nuditi enostavne in celovite rešitve za dostop do storitev znotraj meja domače organizacije in izven njih.

### Kaj AAI-infrastruktura omogoča?

Enotna infrastruktura za overjanje istovetnosti in avtorizacijo vzpostavlja okolje, ki omogoča deljenje aplikacij in znanja med raziskovalno-izobraževalnimi organizacijami, ki so pridružene v slovensko izobraževalno federacijo ArnesAAI. Preverjanje istovetnosti uporabnikov ter hranjenje njihovih osebnih podatkov se izloči iz aplikacij (serviceProvider) in se izvaja na domači organizaciji uporabnikov (IdentityProvider).

ArnesAAI omogoča vzpostavitev enotne, centralizirane zbirke uporabniških podatkov v raziskovalno-izobraževalnih ustanovah. Takšni podatki na organizacijah običajno že obstajajo in jih je treba le ustrezno strukturirati. Tehničnemu osebju to poenostavlja dodeljevanje dostopa svojim članom

(študentom, učiteljem, zunanjim sodelavcem), njihove podatke pa vnesejo zgolj enkrat.

Organizacije lahko funkcionalnosti svojih aplikacij delijo tudi z uporabniki drugih organizacij ali pa svojo enotno zbirko uporabniških podatkov uporabijo za prijavo v lastne aplikacije (npr. spletne učilnice). Uporaba AAI-prijave je mogoča tudi na virtualnih strežnikih (GVS). Paket Polni omogoča AAI-prijavo v Moodle in Joomla, paket Asistenca pa vsebuje vse potrebne komponente, da je tovrstna prijava mogoča tudi v aplikacijah, ki jo podpirajo. Ob vzpostavitvi infrastrukture omrežja Eduroam lahko organizacija uporabi isto zbirko uporabniških podatkov in tako svojim članom ponudi možnost uporabe tega izobraževalnega omrežja.

Končnim uporabnikom ArnesAAI omogoča uporabo enotnega uporabniškega imena in gesla za dostop do vseh storitev, ki jih nudi njegova domača organizacija (npr. spletne učilnice), kot tudi tistih, ki jih nudijo druge organizacije (npr. videokonference VOX, filesender, blog, **Web of Science**). Če ima organizacija vzpostavljeno infrastrukturo za omrežje Eduroam, lahko uporabljajo tudi brezžično omrežje Eduroam v Sloveniji ali tujini.

Ob prijavi v aplikacije se preverjanje pristnosti uporabnika vedno izvede na prijavnem strežniku domače organizacije. Spletna aplikacija nikoli ne vidi uporabnikovega gesla in pridobi vpogled zgolj v tiste osebne podatke uporabnika, ki so potrebni za nudenje storitve. Uporabnik ima ob prijavi popoln nadzor nad prenosom osebnih podatkov in lahko, če aplikaciji ne zaupa povsem, postopek prekliče.

Uspešna preverba pristnosti uporabnika je veljavna določeno časovno obdobje, kar pomeni, da se v tem časovnem obdobju pri dostopu do aplikacij prijava izvede samodejno, brez posredovanja uporabnika. Obdobje je odvisno od nastavitve prijavnega strežnika, lahko le nekaj ur, lahko pa cel dan.

### **Načini pridružitve v ArnesAAI**

Organizacije se lahko v Slovensko izobraževalno raziskovalno federacijo ArnesAAI pridružijo na več načinov, prav tako lahko uporabniki, če njihova organizacija ni članica federacije ArnesAAI, vseeno pridobijo uporabniško ime, ki jim nudi omejene funkcionalnosti.

### **Vzpostavitev lastne infrastrukture na organizaciji**

Takšno uporabo ArnesAAI priporočamo večjim organizacijam in tistim, ki že imajo Eduroam in s tem bazo uporabnikov. Takšen primer so šolski centri, univerze in podobni, ki lahko nastopajo kot skupen ponudnik identitet (IdP) za vse svoje članice. Organizacija potrebuje nekoga, ki jim infrastrukturo vzpostavi in vzdržuje, potrebna pa je tudi relativno hitra in zanesljiva povezava v internet.

### **Gostovanje LDAP + IdP+ RADIUS**

Gostovanje na Arnesu je namenjeno manjšim organizacijam in organizacijam s slabšo infrastrukturo. Organizacija potrebuje nekoga, ki bo s pomočjo LDAP-urejevalnika urejal njihove uporabnike. Sama rešitev je ekvivalent vzpostavitvi lastne infrastrukture na organizaciji, organizaciji pa precej olajša vzpostavitev in vzdrževanje.

### **guest.arnes.si NetID**

Guest.arnes.si NetID je zasilni izhod za vse, ki drugje ne morejo pridobiti uporabniškega imena (NetID). Uporabnost tega uporabniškega imena je omejena, saj uporabniki s tem uporabniškim imenom ne bodo mogli dostopati do določenih vsebin.

### **test.arnes.si NetID**

Trenutno nadomešča guest.arnes.si, ki je opisan v prejšnji točki. V prihodnje bo takšno uporabniško ime (NetID) namenjeno tehničnemu osebju organizacij, ki skrbi in testira AAI-infrastrukturo na organizaciji.

### **Zaključek**

Enotna infrastruktura za overjanje istovetnosti in avtorizacijo (AAI) je odlična alternativa izdajanju novih uporabniških imen in gesel ob vsaki novi storitvi ter ponuja dobre možnosti za medorganizacijsko sodelovanje. Z uvedbo AAI-infrastrukture organizacija močno poenostavi upravljanje z uporabniškimi podatki in svojim uporabnikom zagotovi enostavno uporabo storitev znotraj meja domače organizacije in izven njih.

### **Viri**

1. Papež. Rok. 2008. Enotna prijava v spletne aplikacije. Ljubljana.
2. Arnes. 2012. ArnesAAI – vstopna stran. Dostop: aai.arnes.si (25. 1. 2012).