Tomi Dolenc,
Arnes

Z verodostojno e-identiteto do storitev
Your trusted e-identity – a key to services

Povzetek

Na voljo vam je vedno več storitev in tudi Arnes v zadnjem letu ponuja kar precej novega. Pogosto pa se niti ne zavedate, da geslo za uporabo teh novih storitev verjetno že imate. »Zvijača« je v tem, da tudi v Sloveniji vedno več institucij (vse univerze, kar nekaj šol ...) podeljuje svojim članom oz. uporabnikom e-identitete, ki jih »priznavajo« različne storitve na podlagi skupnega modela (t. i. AAI). Če sami takšne e-identitete še nimate, jo boste verjetno dobili jutri. Danes pa lahko za dostop do teh storitev preprosto uporabite Arnesovo uporabniško ime na nov način.

Ključne besede: E-identiteta, federacija, ArnesAAI, storitve, enotna prijava.

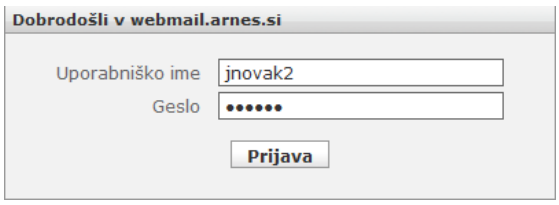
Abstract

More and more services are available, and in the last year ARNES too has had much new to offer. People often don't even realise that they already have a password to access these new services. The “point” is that institutions in Slovenia (all universities, quite a number of schools) increasingly allocate e-identities to their members and users that are “recognised” by various services on the basis of a shared model (i.e. AAI). If you still don't have such an e-identity, you'll probably get one tomorrow. Today you can simply use your ARNES user name in a new way to access these services.

Key words: E-identity, federation, ArnesAAI, services, single-sign-on.

Kako do (spletne) storitve, ki zahteva prijavo?

Odgovor na vprašanje v naslovu je videti banalen: seveda, nekam – najbrž v ustrezno okence (slika 1) – je treba vpisati uporabniško ime (ali nekaj podobnega) in geslo, pa je.



SLIKA 1: TIPIČNA PRIJAVA V SPLETNO APLIKACIJO.

Preden to storimo prvič, je treba najbrž opraviti registracijo, ob kateri ponudniku storitve posredujemo nekaj svojih podatkov, v zameno pa dobimo zgoraj omenjeni »ključ« za uporabo. Od vrste storitve in ponudnika je odvisno, kako zapleten in formalen je postopek registracije. In to je v grobem to.

Ali gre tudi drugače?

V prispevku bomo pojasnili simpatičen koncept, ki želi uporabnikom zmanjšati število potrebnih gesel za različne storitve, ponudnikom pa prihraniti breme registracije. Vse skupaj temelji na pojmu verodostojne e-identitete, ki jo pridobimo

oz. že imamo »doma«, torej nekje, kjer nas že poznajo in se nam torej ni treba ponovno registrirati.

Koncept ni nov in ga največkrat povezujemo s pojmi »federated services« in AAI (Authentication and Authorization Infrastructure). Tokrat se bomo pri njegovi obravnavi osredotočili na perspektivo uporabnika – odtod nekoliko vzgojni ton prispevka[2] – in pri tem skoraj v celoti obšli razlago tehnologije, ki je potrebna za delovanje takšnega sistema.

Pri branju se vam morda razkrije, da imate že danes v rokah ključ do nekaterih novejših storitev, ne da bi se tega zavedali. Preden pa postopek prijave praktično opišemo, bomo pojasnili zamisel sistema in pojme, ki nastopajo v njem.

E-identiteta

Pojem elektronske identitete je širše gledano nek nabor podatkov o posamezniku, ki se uporablja pri dostopanju do omrežnih virov oz. storitev. V tem prispevku bomo z izrazom »e-identiteta« največkrat označevali kar konkretno oznako (identifikator), s katero kot uporabniki v e-svetu izkazujemo svojo istovetnost. Leto je lahko uporabniško ime, ki smo ga pridobili od ponudnika, digitalni certifikat, vpisna številka študenta, profil v družbenem omrežju (npr. na Facebooku). Te identitete imajo različno stopnjo verodostojnosti in tudi uporabljamo jih za različne namene. Težava z njimi je med drugim ta, da jih je vedno več.

Seveda ni verjetno, najbrž pa tudi nesmiselno ali varno, da bi lahko kar eno samo od teh identitet uporabili za vse različne namene. Vendar bi vseeno radi to zmedo nekoliko zmanjšali. Ena očitna pot je, da uporabljamo več storitev istega ponudnika in upamo, da zanje zadošča ena e-identiteta, ki nam jo je ta ponudnik dodelil (pomislimo npr. na velike ponudnike, kot sta Google in Microsoft, ki ponujata celo paleto različnih storitev, ali Arnes v slovenski izobraževalno-raziskovalni skupnosti). Mnoge storitve so takšne, da jih bolj kot verodostojnost identitete uporabnika zanima, kako lahko identitete (in obnašanje) posameznika med seboj povežejo in poleg možnosti registracije dopuščajo ali celo spodbujajo prijavo z obstoječo e-identiteto (»Prijavi se s svojim Facebook profilom!«). Spletne banke npr. *niso* primer takšnih storitev, saj morata obe strani zanesljivo vedeti, s kom imata opravka; pri dostopu do takšnih storitev se zato uporabljajo identitete, overjene s certifikati.

Federacija in verodostojna e-identiteta

Omejimo se nekoliko na svoje delovno oz. učno okolje. Pri svojem delu dostopamo do različnih virov in uporabljamo vrsto storitev, ki so nam dodeljene na podlagi pripadnosti instituciji ali naše delovne vloge v njej (raziskovalec, profesor, študent). Primeri takih storitev so npr. vse, ki sestavljajo delovno okolje – morda prijava v računalnik ali lokalno brezžično omrežje, vstop v spletno učilnico, dostop

[2] Obstaja prepričanje, da se uporabniki – torej ljudje, ki uporabljajo (spletne) storitve – bojijo novosti in da jim je treba vsako stvar potrpežljivo razložiti. Ton razlage, ki so ga vajeni iz šole, naj bi jih zazibal v hipnotičen občutek varnosti, v katerem bodo pojasnilo, kot nekoč v šoli, zlahka sprejeli. Ta predpostavka je iz več razlogov napačna pa tudi če bi držala, je do uporabnikov podcenjujoča, zato je omenjeni ton moč uporabljati le kot stilsko figuro z ustreznim opravičilom ☺.

do člankov in oddaljenih baz podatkov, prijava na izpite, storitve Arnesa ... Vse takšne storitve zahtevajo določeno stopnjo verodostojnosti pri prijavi, saj so bodisi namenjene določeni uporabi (znotraj institucije ali pri sodelovanju s sorodnimi), vezane na pogoje pogodbe z našo matično institucijo (dostop do oddaljenih vsebin) ali ponujajo posebne pogoje glede na status (npr. popust oz. brezplačna uporaba za študente).

Ob tem pa praviloma takoj ob prihodu v to svoje okolje dobimo vsaj eno e-identiteto za uporabo storitev, ki so v bistvu naša delovna (e-)orodja – torej geslo za omrežje, za vstop v spletno učilnico, za izpite ... Ta identiteta je verodostojna znotraj institucije, saj le-ta ve, komu jo je podelila.

Izhodišče za razvoj koncepta »federacije« oz. povezovanja različnih storitev v enotnejšo uporabniško izkušnjo je sedaj preprosto: zakaj ne bi za vse ali vsaj čimveč teh storitev, ki sestavljajo naše delovno okolje, uporabili iste e-identitete (ki jo že imamo oz. jo moramo pridobiti takoj, ko želimo uporabljati e-storitve v svojem okolju)?

Da koncept deluje, je potreben *dogovor:* uporabnik je – na neki standardiziran način – registriran in dobi *e-identiteto* na enem mestu, naravno oz. praviloma je to njegovo delovno okolje oz. matična institucija (fakulteta, šola), ki njegovo identiteto pozna in je torej ni treba dodatno preverjati. Ta institucija nastopa kot *ponudnik (in tudi varuh) identitete* svojega člana – uporabnika storitev. Storitev (oz. ponudnik, ki za njo stoji) pa mora, namesto da bi zahtevala registracijo, sprejeti e-identiteto uporabnika in verjeti njeni verodostojnosti. Ker za verodostojnost jamči matična organizacija, le-ta kot *ponudnik identitete* sklene s *ponudnikom storitev* ustrezen dogovor in se tako z njim poveže v zvezo (federacijo).

Vse to dogovarjanje seveda uporabnika bolj malo zanima: zanj je pomembno le, da dobi »geslo«, ki je uporabno za čim več e-orodij, ki jih pri svojem delu potrebuje.

Vse lepo in prav, vendar ali tudi deluje?

Iz zgoraj povedanega je razvidno, da so za delovanje koncepta – poleg dogovora, ki v resnici pride na koncu – potrebne naslednje komponente: nekakšna infrastruktura, ki vse skupaj povezuje, ustrezno upravljanje identitet in seveda primerno število storitev, ki tak dogovor upoštevajo.

E-infrastruktura (middleware)

Za izobraževalno-raziskovalno okolje uvajajo evropska in svetovna nacionalna omrežja, kakršno je Arnes, enotno programsko infrastrukturo (AAI, aai.arnes.si), ki omogoča delovanje koncepta federacij. Slovenska izobraževalna federacija ArnesAAI je del te infrastrukture, sorodna je tudi federacija Eduroam (eduroam.arnes.si), ki povezuje brezžična omrežja predvsem univerz po Evropi in tudi izven nje, uporabnikom pa ponuja preprost dostop v omrežje z enotnim geslom na katerikoli od članic federacije. Arnes vzdržuje programsko infrastrukturo in upravlja obe federaciji ter pri tem ponuja pomoč pri vključevanju v federacijo in gostovanje ustreznih strežnikov.

Upravljanje identitet

Matična institucija oz. ponudnik identitete mora ustrezno upravljati identitete uporabnikov (skrbeti za ažurnost, za distribucijo e-identitet svojim članom), kar načeloma ne bi smelo biti pretežko, saj že zdaj upravlja vsaj eno (verjetno pa več) registrov svojih članov za najrazličnejše namene. Seveda pomaga, če imamo za to primerna orodja. V sodelovanju z Arnesom se v okviru projekta E-šolstvo razvija orodje, ki bo to upravljanje olajšalo vsaj slovenskim srednjim in osnovnim šolam, verjetno pa bo uporabno tudi širše (Podbrščček, 2012).

Storitve

Število storitev, ki so dostopne na ta način, se povečuje. Vsekakor so v slovenskem raziskovalnem in izobraževalnem okolju to vse novejše Arnesove spletne storitve – *Filesender* (filesender.arnes.si), *Arnes Blog* (blog.arnes.si), *spletne konference VOX* (vox.arnes.si) – ki zahtevajo identifikacijo uporabnika in mu morda na podlagi njegovega statusa (učitelj, dijak) tudi določijo različne pravice.

Danes na Arnesu vse spletne storitve razvijamo tako, da bi bile preko ArnesAAI takoj dostopne vsem upravičenim uporabnikom na univerzah, v šolah in drugih organizacijah brez zamudnih postopkov s prijavnicami in potrjevanjem statusa. Novost v letu 2012 je npr. spletna aplikacija, ki vsem imetnikom veljavne e-identitete v federaciji ArnesAAI omogoča, da si na Arnesovem strežniku pridobijo nekaj lastnega prostora in odprejo svoj poštni predal, kar je bilo doslej mogoče le s »papirno« registracijo (Vreča, 2012).

Ker gre pri AAI za standardne in razširjene protokole, se mnoge tipične spletne aplikacije, uporabne v izobraževalnem okolju (npr. spletne učilnice Moodle) preprosto prilagodijo temu načinu prijave.[3] Prilagojene so mu tudi storitve, ki nastajajo v okviru projekta E-šolstvo (www.sio.si). Možnost prijave preko AAI brez težav upoštevamo pri razvoju novih storitev in tako sledimo cilju, da bi za čim več vsakodnevnih opravil potrebovali le eno geslo. Če le gre, je smiselno prilagoditi tudi že obstoječe aplikacije.

Prav tako pa lahko mnogi veliki ponudniki (založbe z online bazami podatkov, Google, Microsoft) ponudijo svoje storitve na ta način, če z njimi sklenemo ustrezen dogovor (gl. npr. (Arnes, [2])).

Tipični elementi e-identitete v federaciji

Identifikatorju oz. e-identiteti, s katero se prijavimo v neko storitev, pogosto rečemo *uporabniško ime* (username, UserID) in je po navadi sestavljena iz niza znakov (lahko tudi številk), ki nam ga dodelijo ob registraciji ali pa si ga lahko izberemo sami. To ime nas enolično določa znotraj storitve oz. organizacije, pri kateri smo registrirani.

Vsi ponudniki storitev, pridruženi določeni federaciji, prepoznajo vse e-identitete uporabnikov, ki prihajajo od kateregakoli ponudnika identitet. Verodostojna e-identiteta v federaciji je sestavljena iz dveh delov: t. i. »kraljestva« (realm), ki

[3] Za gostujoči Moodle v paketu »Polni« opravi to prilagoditev Arnes, gl. (Arnes, [1]).

pripada ponudniku identitet in združuje določeno skupino uporabnikov (en ponudnik lahko pokriva več kraljestev) ter uporabniškega imena, ki ga ponudnik dodeli vsakemu posameznemu uporabniku v svojem kraljestvu. E-identiteta, ki bi ji lahko rekli tudi »enotno uporabniško ime v federaciji AAI«, je torej sestavljena takole:

e-identiteta == Kdo + OdKod

ali zapisano drugače: NetID == UserID@Kraljestvo

Pri tem smo za »tehnično« oznako tega identifikatorja izbrali ime NetID, da poudarimo veljavnost razširjenega uporabniškega imena (UserID) v omrežju federacije. Kraljestvo pa ustreza kar eni od veljavnih internetnih domen, ki pripada ponudniku identitete. Primeri veljavnega NetID bi lahko bili naslednje oblike[4]:

jnovak2@neka.sola.si

janez.novak@pef.uni-lj.si

123456789@student.uni-lj.si

Opazimo, da je NetID po obliki zelo podoben naslovu za e-pošto. Opozorimo, da tu nastopa v drugi vlogi, prav tako ni nujno (celo praviloma ne), da bi NetID ustrezal nekemu dejanskemu naslovu e-pošte. Sicer pa nas ta dvojnost med uporabniškim imenom in e-naslovom ne bi več smela begati (prim. npr. prijavo v Google).

Ponudniki identitet v federaciji ArnesAAI

V federacijo ArnesAAI so vključene vse slovenske univerze, naraščajoče število šol in nekatere druge organizacije (mnogi so hkrati vključeni tudi kot ponudniki storitev, npr. lastnih spletnih učilnic, gl. http://aai.arnes.si/seznam.html). Vsi ti lahko svojim uporabnikom izdajo veljavno identiteto, ki jim med drugim omogoča uporabo vseh Arnesovih storitev, ne da bi za to morali registrirati uporabniško ime na Arnesu, za kar je sicer potreben postopek s potrjeno prijavnico. Večinoma so te organizacije tudi članice federacije Eduroam, zato praviloma velja isti NetID tudi za dostop do brezžičnega omrežja Eduroam doma in po svetu.

Gostujoča e-identiteta na Arnesu

Vsaka organizacija, ki želi svojim uporabnikom ponuditi dostop do storitev v federaciji ArnesAAI, mora torej najprej vzpostaviti standardiziran imenik svojih članov in ustrezen strežnik,[5] ki uporabniku omogoča prijavo na domači organizaciji. Da bi pri tem pomagali, smo na Arnesu omogočili gostovanje takšnih imenikov/strežnikov, organizacija mora torej poskrbeti le za ažuriranje podatkov.

[4] Zadnja dva primera prikazujeta kraljestvi, ki najbrž pripadata istemu ponudniku identitete (univerzi).

[5] Tak strežnik v e-svetu prav tako imenujemo »ponudnik identitete« oz. (Identiy Provider) in ga navadno označujemo s kratico IdP.

Da pa bi dostop do storitev omogočili tudi tistim uporabnikom, katerih matična organizacija (še) ni članica ArnesAAI, lahko imetniki uporabniških imen na Arnesu[6] uporabijo tudi ustrezno nadomestno ali gostujočo e-identiteto v federaciji ArnesAAI. Ta e-identiteta predstavlja razširitev uporabniškega imena (username) in ima obliko

NetID == username@guest.arnes.si

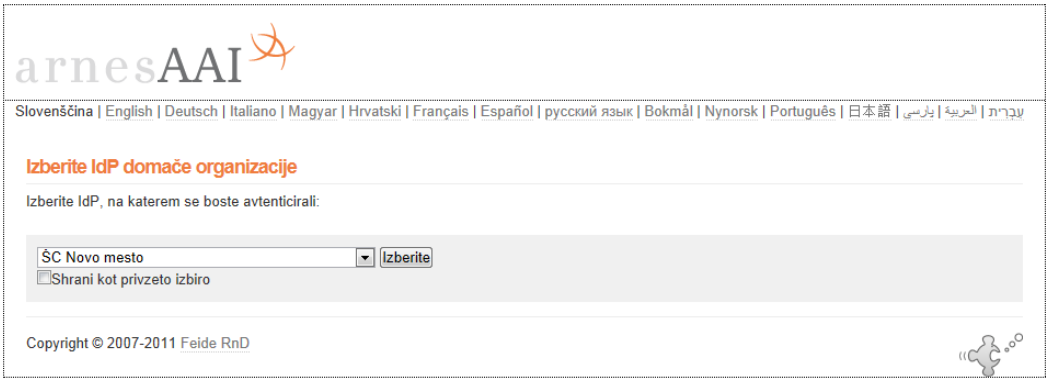
Tako se lahko npr. Janez, ki ima na Arnesu uporabniško ime »*jnovak2*«, predstavlja v federaciji ArnesAAI kot »*jnovak2@guest.arnes.si*«. Domena jasno nakazuje, da gre za gostujočo e-identiteto, zato tak uporabnik morda ne more izkoristiti vseh funkcionalnosti neke storitve, ki bi bile vezane na njegovo pripadnost določeni organizaciji. Vsekakor lahko uporablja storitve Arnesa, drugi ponudniki storitev pa mu lahko omogočijo uporabo pod svojimi pogoji.

Nova uporabniška izkušnja

Ker se storitve v federaciji AAI zanašajo na obstoječe e-identitete, je uporabniška izkušnja ob prijavi nekoliko drugačna, kot smo je vajeni oz. kot je opisana v uvodu, zato morda sprva deluje kot ovira. Zavedati se moramo, da nas storitev »ne pozna« – ne more preveriti našega gesla, zato se vedno najprej prijavimo svojemu *ponudniku identitete*, ki hrani naše podatke. Pri tem mu dovolimo, da storitvi posreduje tisti del naših podatkov, ki so za delovanje storitve potrebni; šele potem smo v storitev prijavljeni. Vendar pa se ob novih prijavah deli postopka preskakujejo, saj smo jih že opravili! Oglejmo si ta postopek podrobneje.

Postopek prijave v storitve federacije ArnesAAI

Začnemo torej z izbiro svojega *ponudnika identitete*, pri čemer nam bolj ali manj ustrežljivo pomaga vmesnik z menijem, kjer so našteti vsi člani federacije, ki nastopajo kot ponudniki identitet. Le-to je lahko videti npr. takole (slika 2):



SLIKA 2: PRVI KORAK PRIJAVE: IZBOR PONUDNIKA IDENTITETE

Ponudnik identitete pri tem pomeni organizacijo – načeloma našo matično, ki nam je izdala e-identiteto, lahko pa tudi Arnes, če uporabljamo gostujočo identiteto. Navodila za pravilno prijavo bomo vedno dobili od ponudnika identitete, torej tistega, od katerega smo e-identiteto (NetID in geslo) prejeli. Ker se bomo

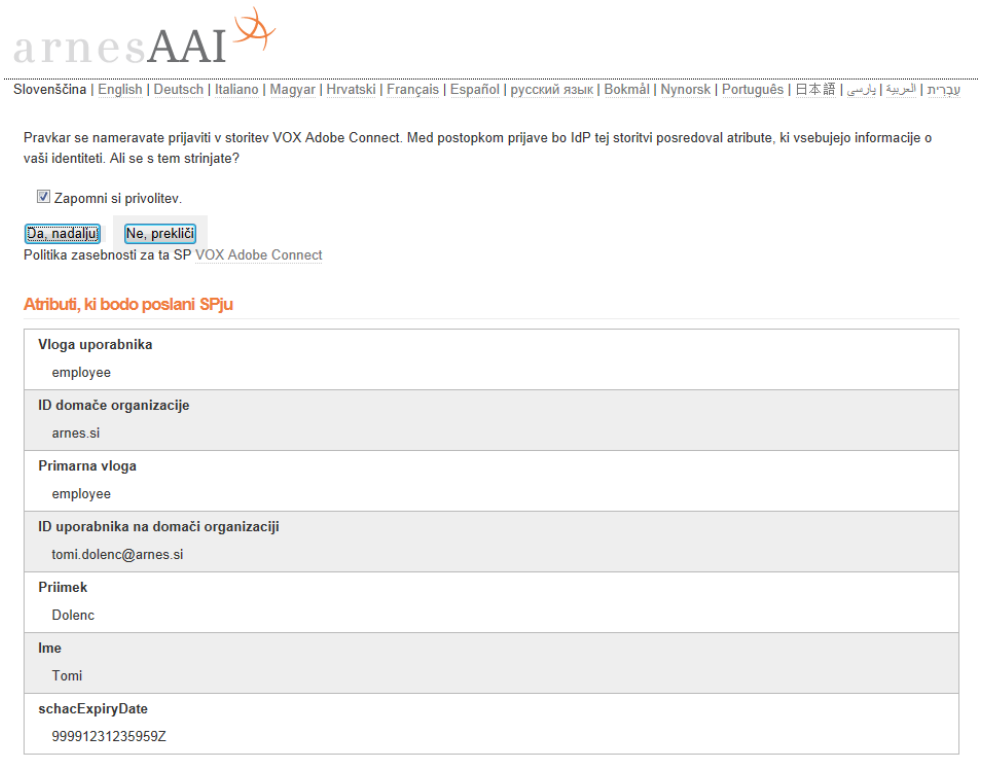
[6] http://www.arnes.si/storitve/storitve-za-posameznike/pridobitev-uporabniskega-imena.html

praviloma prijavili vedno preko istega ponudnika identitete (IdP), lahko nastavimo privzeto izbiro.

V naslednjem koraku se ponudniku identitete predstavimo s svojo e-identiteto, tako da vnesemo svoje »uporabniško ime v federaciji AAI«, torej NetID, in pripadajoče geslo. Primer na sliki 3 prikazuje vmesnik Arnesovega IdP, saj ima avtor svojo
e-identiteto na Arnesu. Vaš ponudnik identitete ima morda malce drugače oblikovan vmesnik.

SLIKA 3: DRUGI KORAK PRIJAVE: VNOS NETID IN GESLA NAŠEMU PONUDNIKU IDENTITETE

Naslednji korak nas vsaj prvič vizualno najbolj »prestraši«, čeprav je prav ta korak ključ do našega popolnega nadzora nad posredovanjem svojih osebnih podatkov posameznim storitvam. Ponudnik identitete (strežnik) nas namreč opozori, katere podatke iz imenika bo posredoval storitvi – praviloma lahko storitev zahteva le tiste podatke, ki jih potrebuje za svoje delovanje. V tem trenutku si lahko premislimo, če menimo, da storitev od nas zahteva preveč osebnih podatkov. Včasih storitvi popolnoma zadošča že sam NetID. Na primeru na sliki 4 lahko vidimo, da storitev VOX poleg NetID zahteva še ime, priimek, vlogo uporabnika v organizaciji (»employee«) ter datum poteka veljavnosti. Na podlagi teh podatkov namreč lahko upravlja z vsebinami, ki jih uporabnik hrani na strežniku.



SLIKA 4: TRETJI KORAK: PRIVOLITEV POSREDOVANJA OSEBNIH PODATKOV STORITVI

Po tem koraku smo v storitev prijavljeni in jo lahko začnemo uporabljati. Postopek je morda videti zapleten v primerjavi z »običajnim« vpisom uporabniškega imena in gesla na spletni strani storitve, vendar kmalu ugotovimo, da je pri večjem številu storitev prijaznejši, saj je ne glede na različne storitve vedno enak in nam tako postane domač, poleg tega pa se privzete izbire shranijo (gl. tudi sliko 3) in nam pri vseh naslednjih prijavah občutno skrajšajo pot. Zares pa nas razveseli to, da se nam naenkrat v različne storitve sploh ni treba več prijavljati, če smo že enkrat opravili prijavo s svojo e-identiteto, saj za storitve federacije velja načelo *enotne prijave* (Single-Sign-On), dokler se pač ne odločimo, da je za danes dovolj in se odjavimo.

Zaključek

Namen tega prispevka je trojen. Prva želja je bralca dovolj obširno in razumljivo seznaniti z vlogo in pomenom njegove nove e-identitete (NetID), ki predstavlja razširitev pojma uporabniškega imena, ki nam ga dodeli ponudnik (bodisi matična organizacija ali ponudnik gostujočih identitet). Ta e-identiteta namreč »velja« pri več različnih ponudnikih storitev v federaciji. Drugi je seznaniti imetnike ali upravičence do Arnesovega uporabniškega imena o novi funkcionalnosti (»moje uporabniško ime je lahko NetID«). Tretji pa je opozoriti vse imetnike veljavnih (ali bodočih) e-identitet v federaciji ArnesAAI na storitve, ki so jim na voljo, ne da bi zanje potrebovali nova gesla oz. registracijo.

Viri

1. Podbršček, M., (2012): Upravljanje z identitetami. V: Mednarodna multikonferenca Splet izobraževanja in raziskovanja z IKT – SIRikt 2012 (zbornik),Kranjska Gora 21. – 24. marec 2012. Ljubljana: Miška d.o.o.

2. Vreča, M., (2012): Nov osebni paket – naklikaj si svoj e-mail. V: Mednarodna multikonferenca Splet izobraževanja in raziskovanja z IKT – SIRikt 2012 (zbornik),Kranjska Gora 21. – 24. marec 2012. Ljubljana: Miška d.o.o.
3. Arnes, [1]: http://www.arnes.si/storitve/splet-posta-strezniki/dinamicno-gostovanje-phpmysql/paketi/polni.html (2011).
4. Arnes, [2]: http://www.arnes.si/obvestila/obvestilo/article/dostop-do-bibliografskih-baz-podatkov-web-of-science-tudi-z-arnesaai.html (8. 4. 2011).