Milan Podbršček, TŠCNG

Upravljanje z e-identitetami
Identity managemet

Povzetek

Povezovanje storitev v zadnjem času vedno pogosteje rešujemo z imeniki (LDAP in AD, znotraj organizacije) in AAI-jem (zunaj organizacije). Upravljanje z identitetami znotraj imenikov ni enostavno rešljivo, zato smo se odločili razviti spletno aplikacijo, ki nam bo v pomoč pri tem delu. Kot dodano vrednost lahko aplikacija nudi vir podatkov o učečih in njihovih starših ter zaposlenih tudi drugim aplikacijam, ki jih uporabljamo pri našem delu.

Ključne besede: e-identiteta, LDAP, AD, infrastruktura

Abstract

In recent times, it has become increasingly common to link services using directories (LDAP and AD, within organisations) and AAI (outside organisations). Identity management within directories is not a trivial task, so we decided to develop a web application to make it easier. As added value, the application can provide a source of data on learners, parents and employees for other applications that we use in our work.

Key Words: e-identity, LDAP, AD, infrastructura

Uvod

Za uporabo storitev v poslovnem okolju in v spletu se mora uporabnik identificirati. Imeti mora uporabniški račun, ki je v večini primerov sestavljen iz uporabniškega imena in gesla. Le za nekatere storitve je prijava okrepljena z uporabo certifikatov (ravnateljski portal na MŠŠ, banke ipd.) ali gesel za enkratno uporabo (OTP – angl. One Time Password). Ker si je težko zapomniti množico uporabniških imen in gesel, bi uporabniki radi za več storitev uporabili isto identiteto (uporabniško ime in geslo).

Vzgojno-izobraževalni zavodi (v nadaljevanju VIZ) niso nobena izjema. Uporabljajo različne aplikacije za upravljanje procesov v šoli. Posplošeno lahko rečemo, da šole uporabljajo dve ključni kategoriji aplikacij:

1. aplikacije za spremljanje pedagoškega procesa
2. aplikacije za vodenje računovodsko/knjigovodsko-kadrovskega procesa

Ključne aplikacije so Lopolis in e-Asistent za spremljanje pedagoškega procesa ter SAOP in Vasco za vodenje računovodstva oz. knjigovodstva.

Lopolis kot primarna aplikacija za vodenje pedagoškega procesa je še posebej “močna” oz. pogosta v osnovnih šolah. V srednjih šolah se vedno bolj uveljavlja e-Asistent, zaslediti je mogoče tudi lastne rešitve, in sicer predvsem na informacijsko razvitejših šolah. Vsaka od aplikacij zahteva določene podatke, ki so enaki ali pa zelo podobni in bi lahko bili poenoteni.

Poleg upravljanja zgoraj navedenih procesov v zadnjem času na šolah vse pogosteje uporabljamo tudi sisteme za upravljanje z učnimi vsebinami (npr. Moodle) in sisteme za upravljanje z vsebinami (npr. Joomla). Vedno več je tudi različnih spletnih aplikacij, ki jih ponuja Arnes. Tudi te aplikacije potrebujejo zbiranje in vodenje povsem istih ali podobnih podatkov kot sistemi za upravljanje šole. Poleg tega te aplikacije zahtevajo vodenje uporabniških imen in gesel. Določene Arnesove storitve potrebujejo tudi podatke o preteku vpisa učenca/dijaka ter vlogo zaposlenega na šoli.

Rešitev

K reševanju problema bomo pristopili z dveh nivojev, eden je znotraj posamezne organizacije, drugi je povezan navzven.

Pod povezovanjem navznoter[1] razumemo povezovanje aplikacij znotraj šole. Aplikacije se bodo povezovale na skupno bazo, za katero skrbi sistem za upravljanje z identitetami (v nadaljevanju IdM). Iz njega bodo pobirali podatke različni imeniki, kot sta na primer imenika LDAP (Lightweight Directory Access Protocol) ali Microsoft AD (Active Directory), in aplikacije, ki so namenjene upravljanju učnega procesa in upravljanju poslovanja. Za imenike je razvit »push« način, način dela z drugimi aplikacijami pa je odvisen od aplikacij samih. Pripravljena je shema, po kateri bodo lahko te aplikacije dostopale do podatkov.

Spletne aplikacije na področju dela pri pouku se lahko povežejo na imenike (LDAP, AD). Nekatere aplikacije v upravnem procesu se ravno tako že povezujejo na obstoječe imenike. Za mnoge podatke, ki so v imenikih, ne zadostujejo, zato lahko pričakujemo, da se bodo povezale raje na IdM.

Pod povezovanjem navzven[1] razumemo povezovanje na aplikacije, ki niso v lasti šole, torej predvsem storitve, ki jih vzgojno-izobraževalnim zavodom nudi Arnes. Le-to je rešeno na nivoju AAI-ja[3] in ni predmet te razprave, čeprav AAI uporablja določene šolske imenike (LDAP in AD).

Predstavitev

Sistem za upravljanje z identitetami[4] je spletna aplikacija. Je odprtokodna rešitev, ki za bazo uporablja FireBird. V spodnji tabeli so našteti vsi atributi, ki jih vodi.

Uporabniški račun	Osebni podatki	Kontaktni podatki
Uporabnisko_Ime Uporabnisko_Ime_Polno Geslo St_Prijav St_Neuspesnih_Prijav St_Neuspesnih_Prijav_Sum St_Menjav_Gesla St_Ponastavitev_Gesla Datum_Prva_Prijava Datum_Zadnja_Prijava Datum_Zadnja_NeuPrijava Datum_Zaklenjeno Datum_Menjava_Gesla Datum_Ponastavitev_Gesla	Ime Priimek Priimek2 Spol EMSO Davcna_ST Datum_Rojstva Drzavljanstvo_ID Drzava_Rojstva_ID Kraj_Rojstva_ID Kraj_Rojstva	Telefon_Mobilni Telefon_Doma Telefon_Sluzba Email

Datum_Potek_Gesla Datum_PozGeslo_SKLIC		

Lokacijski podatki	Podatki učečega	Podatki učečega – razred	Podatki učečega – VIZ-program
Ulica Hisna_ST Posta_Kraj_ID Kraj Posta_ID Zacasno_Ulica Zacasno_Hisna_ST Zacasno_Posta_Kraj_ID Zacasno_Kraj Zacasno_Posta_ID	VPISNA_STEVILKA UDELEZENEC_ID_MSS DATUM_ZAVOD_VPISAN_OD DATUM_ZAVOD_VPISAN_DO DATUM_ZAKLJUCKA_IZ ZAKLJUCNA_STOPNJA_GL	RAZRED_LETNIK_ID DATUM_VPISAN_OD DATUM_VPISAN_DO NACIN_IZOBRAZEVANJA_ID STATUS_UDELEZBE_ID OBLIKA_IZOBRAZEVANJA_ID POVPRECNA_OCENA	VIZ_PROGRAM_ID DATUM_VPISAN_OD DATUM_VPISAN_DO

Namenjen je upravljanju podatkov učencev/dijakov, njihovih staršev in zaposlenih. Zajem podatkov je mogoč z masovnim ali individualnim vnosom. Mogoče je urejanje vseh podatkov (seveda glede na pravice posameznika). Trenutno so implementirani štirje nivoji varnosti[2] in s tem seveda tudi funkcije posameznika, kot jih ima v poslovnem procesu. Vzdrževalec sistema (root) lahko vidi in ureja vse podatke. Šolski upravljavec lahko vidi in ureja podatke svoje šole, urednik pa lahko ureja zgolj podatke o učencih/dijakih, starših in zaposlenih.

Vsak posameznik/uporabnik, ki je vključen v IdM, lahko vidi svoje podatke, nekatere med njimi lahko tudi popravi. Predvsem je tu mišljena sprememba gesla. Pomembna funkcija je ponastavitev pozabljenega gesla, poleg tega pa lahko vsak posameznik vidi tudi zgodovino sprememb svojih podatkov.

Spremenjeni podatki se sinhronizirajo s podatki v LDAP-u in AD-ju. Sistem omogoča izvoz podatkov v XML- in XLS-format. Dolgoročno je načrtovano tudi omogočanje neposrednega zajema (push ali pull) podatkov drugim aplikacijam. Prenosi podatkov se izvajajo s šifriranimi povezavami.

Zaključek

Z razvojem sistema za upravljanje z identitetami smo močno olajšali delo šolskemu osebju, ki skrbi za različne evidence, izrazito pa je olajšano tudi delo informatikom, ki skrbijo za uvajanje novih storitev v šolsko okolje. Uporabnikom smo zmanjšali število uporabniških imen in gesel.

Seveda to ni konec razvoja. Veliko bo treba narediti še na različnih izpisih in v prihodnosti tudi na uporabi osebnih certifikatov za povečano varnost dostopa do sistema.

Viri in literatura

1. Linden Mikael, Organisational and cross organizational identity management, Tempere univesity of Technology, pulication 779, Tempere 2009
2. Mark Bruhn, Michael Gettes, and Ann West, Identity and Access Management
   and Security in Higher Education,
   http://www.educause.edu/ir/library/pdf/eqm0342.pdf,
3. Avgust Jauk, AAI v slovenskem izobraževalno raziskovalnem okolju, http://www.sirikt.si/fileadmin/sirikt/predstavitve/2009/Arnes_federacija.pdf