Návrh použití atributů pro federaci eduID.cz (v2)

Povinné atributy

Každý poskytovatel identit musí být schopen povinné atributy poskytovat, ale nemusí je poskytovat všem poskytovatelům služeb. Jedná se o následující.

urn:mace:dir:attribute-def:eduPersonPrincipalName - (dle eduPerson)
urn:mace:dir:attribute-def:eduPersonScopedAffiliation - (dle eduPerson)
urn:mace:dir:attribute-def:cn – celé jméno v pořadí jméno(jména) a příjmení bez titulů - (dle eduPerson)
urn:mace:dir:attribute-def:eduPersonTargetedID – (dle eduPerson) – zůstává k diskuzi, zda atribut bude umístěn mezi povinné nebo regulované atributy.

Atributy budou plněny v souladu se specifikací eduPerson (http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200712.html) s případným upřesněním pro účely eduID.cz, kde bude potřeba.

Regulované atributy

Všichni poskytovatele identit, kteří používají regulované atributy, je používají pouze k níže uvedenému účelu

urn:mace:dir:attribute-def:givenName – jméno uživatele
urn:mace:dir:attribute-def:sn – příjmení uživatele
urn:mace:dir:attribute-def:ou – označení organizační složky v rámci organizace
urn:mace:dir:attribute-def:o – označení organizace
urn:mace:dir:attribute-def:mail – adresa elektronické pošty uživatele

Výše uvedené atributy slouží pro prezentační účely a není vhodné je používát pro autorizaci.

urn:mace:dir:attribute-def:eduPersonEntitlement – atribut pro řízení přístupu k vyjmenovaným službám (dle eduPerson)

urn:mace:dir:attribute-def:czEduPersonStudySubject – studijní obor dle číselníku MŠMT
urn:mace:dir:attribute-def:czEduPersonStudyProgramme – studijní program dle číselníku MŠMT
urn:mace:dir:attribute-def:eduPersonOrgUnitDN – (dle eduPerson)

Lokální atributy

Lokální atributy vznikají pro účely různých projektů. Obdobně jako atributy regulované se nesmí používat v rámci celé federace k jinému účelu, než k jakému je popsáno. V současné době se jedná o následující.

http://www.mefanet.cz/mefaperson/ - atribut nabývá hodnot lf.muni.cz, lf1.cuni.cz, lf2.cuni.cz, lf3.cuni.cz, lfhk.cuni.cz, lfp.cuni.cz atd. pro zaměstnance a studenty lékařskách fakult. Podrobnosti a aktuální informace jsou na *http://www.mefanet.cz/mefaperson/* .

U výše neuvedených atributů se doporučuje přednostně využívat atributy a jejich definice použité v objektové třídě eduPerson.

Doporučení

Pro autorizaci je vhodné používat zejména atribut *eduPersonScopedAffiliation*, který vystihuje vztah uživatele k organizaci, např. member@organizace.cz. Naopak je nevhodné používat k autorizaci identifikaci IdP.

Při autorizaci podle příslušnosti uživatele k určitým částem organizací, např. při povolení přístupu ke službě A jen zaměstnancům oddělení B z organizace C a studentům předmětu D na univerzitě E, je vhodné zavést na všech zúčastněných IdP novou hodnotu atributu *eduPersonEntitlement* označující uživatele s právem přístupu ke službě A, tj. o autorizaci rozhodovat na IdP. Opačný postup, kdy IdP poskytují informace o vztahu uživatelů k oddělením a zápisu předmětů, a o autorizaci rozhoduje sama služba A, nutí správce služby rozumět vnitřním vztahům ve všech zúčastněných organizacích, což nemusí být vhodné.

Pro zvýšení ochrany osobních údajů uživatelů je vhodné předávat poskytovatelům služeb pouze nezbytný počet atributů a preferovat použití atributu *eduPersonTargetedID*.

26.8.2008, Daniel Kouřil, Martin Kuba, Radim Peša, Michal Procházka