Implementarea Serviciilor Federative în RM

Pocotilenco V.
Universitatea Tehnică din Moldova
Chișinău, Moldova
poco@mail.utm.md

Bogatencov P.
RENAM
Chișinău, Moldova
bogatencov@renam.md

Sclifos C.
Academia de studii Economice din Moldova
Chișinău, Moldova
sclifcon@vle.ase.md

***Abstract* — Contemporary level of scientific and technical development is due to sharing relevant information and in this case it is very important to organize access to various informational systems with protected informational resources. Implementation of right instruments for interaction with informational systems for research and educational communities is a real necessity and will have essential contribution to increase capacity for knowledge.**

Keywords - GEANT, services, PKI, R&E

I. Introducere

Necesitățile și cerințele informaționale contemporane sunt în permanentă creștere. Sursele informaționale accesate pot fi absolut de diferita natură, organizare sau destinație. Ca urmare utilizatorul este nevoit sa folosească multiple seturi de date pentru acces la ele. Pentru simplificarea procesului de utilizare a resurselor informaționale a fost propusa tehnologia SSO (Single Sign On). Avantajele implementării SSO sunt resimțite atât de utilizator cit și de prestatorul de servicii de management al identității.

II. Servicii SSO

Inițial ca o soluție de acces a serviciilor din interiorul unui proiect (fig.1), aceasta tehnologie a fost extinsa pentru a putea facilita accesul la resurse atât distribuite geografic cât și diverse după destinație sau metoda de acces.

Fig. 1 Servicii SSO Microsoft

Pentru necesitățile crescătoare al utilizatorilor au fost elaborate mecanisme și sisteme de management a identității atât pentru diverse modele de acces. Exemplu de mecanisme SSO de acces la nivel local sunt resursele oferite în cadrul unei instituții de învățământ sau cercetări(fig.2)[3]. Un alt exemplu a unui mecanism SSO este accesul către e-resursele naționale aplicând un singur set de date de acces (fig.3), ca exemplu IDNO sau diferite seturi de date pentru fiecare serviciu în parte .

Daca pentru implementarea modelelor descrise mai devreme nu sunt impuse restricții și necesitate de conformare a sistemului AAI, pentru interconectarea resurselor instituționale naționale sau internaționale situația e complet diferita.

Pentru depanarea situației menționate vom considera că exista doua componente de baza:

- IdM –serviciu de management a identității
- SP – servicii, resurse

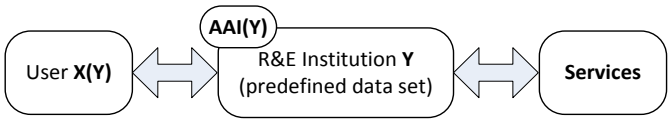


Fig.2 Mecanism SSO instituțional.

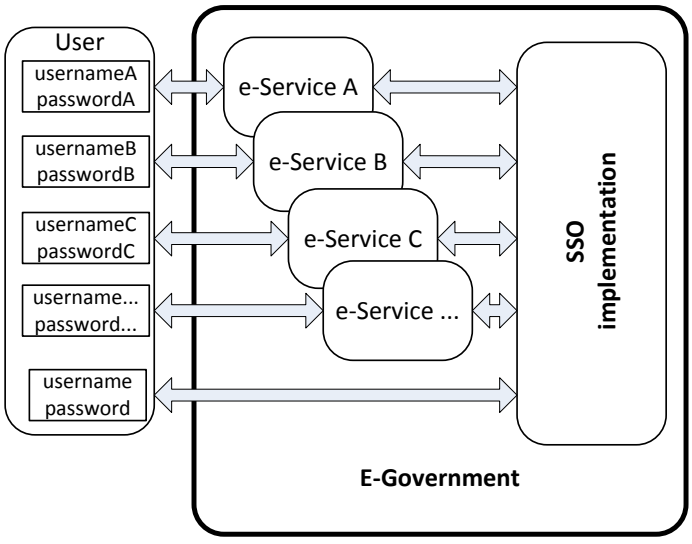
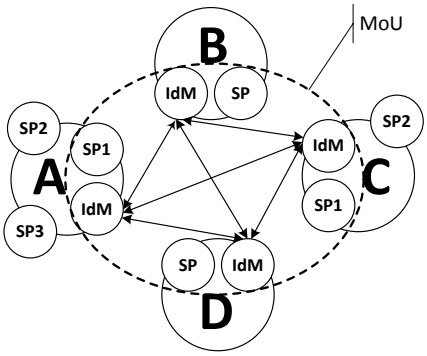


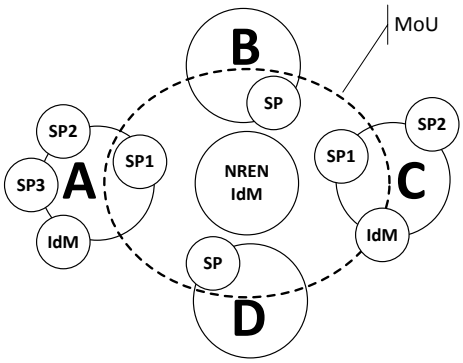
Fig.3 Mecanism SSO național.

Vom considera ca fiecare instituție poate avea minim câte un element IdM și SP(fig.4.a). Aceste instituții aplicând un acord de partajare a resurselor informaționale se vor

conforma la un set de date minim necesar pentru funcționarea efectiva a AAI. In aceasta situație fiecare instituție își păstrează datele în cadrul propriului IdM și autentifica/autorizează solicitările parvenite de la membrii acordului. Astfel de arhitectură este numita mesh. O alta situație poate fi considerata în cazul când IdM este realizat într-o formă centralizata pentru serviciile partajate (fig.4.b), arhitectura fiind numită Hub&Spoke. Astfel de implementare majorează eficacitatea mecanismului de autorizare și simplifică interconectarea resurselor la nivel regional.



a)



b)

Fig.4 Forma de partajare a serviciilor.

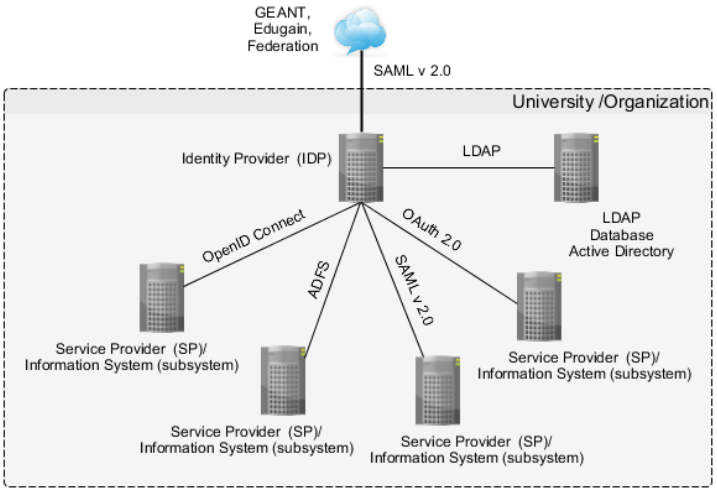
Un alt avantaj al unei astfel de realizări este reducerea costurilor și riscurilor de întreținere a unui IdM. La rândul sau NREN poate conlucra cu organizații similare conformându-și AAI cu cerințele de acces către resurse regionale.

Procesul de grupare a instituțiilor în scop de partajare a resurselor este descris ca proces de creare a *Federatiei*. Acest proces este pe larg susținut în cadrul rețelei pan-Europene *GEANT*[1] prin serviciul *eduGain* și diseminat prin intermediul întrunirilor tematice organizate de *TERENA*.

III. Schimb de Date în Cadrul Federației

Pentru implementarea unei infrastructuri federative cu scopul partajării resurselor și cu serviciul *eduGain* este necesar de ținut cont de metode, cerințe și principii bine determinate, care trebuie executate cu strictețe de către toți membrii acesteia[2]. În cazul *eduGain* ca protocol de bază, pentru schimbul de date, este utilizat SAML v.2.0. aplicarea acestui protocol este necesară până la IdP din cadrul instituției, iar în cadrul organizației și rețelei acestea pot fi utilizate o diferite procedee pentru schimbul de date în dependență de necesitate. Ca exemplu în cazul utilizării Microsoft Active Directory poate fi utilizat ADFS pentru conexiune cu IDP al Service Provider-ului (SP), pentru resurse informatice WEB pot fi utilizate procedee bazate pe OpenID Connect sau OAuth 2.0, pentru autentificare și autorizare(fig.5)[4].

Fig.5 Protocoale utilizate pentru infrastructura federativă.



O latură importantă a securității este punctul de introducere a datelor senzitive în procesul de acces către serviciul selectat. Există 2 căi de acces către serviciile federative (fig. 6)[6].

În dependență de soluțiile middleware pentru transport date SAML, prezentate în fig. 5, accesul către serviciul solicitat poate fi obținut prin:

- *SP initiated login* – în acest caz utilizatorul din instituția B în primul rând va accesa serviciul solicitat (fig. 6a), aflat în instituția A. Evident în instituția A nu exista informație despre utilizator, deci fiind în cadrul *Federației*, SP va "întreba" instanța IdP din instituția B dacă este autorizat utilizatorul să acceseze serviciul, deci se va inițializa procesul de autentificare/autorizare după redirecționarea către IdP. În rezultat utilizatorul va putea accesa serviciul.
- *IdP initiated login* – în acest caz utilizatorul se va loga în instanța IdP din cadrul instituției B, deci va efectua procesul de autentificare. În următorul pas este accesul către serviciu, efectuat după autorizare în cadrul SP instanței.

IV. Proiect Pilot

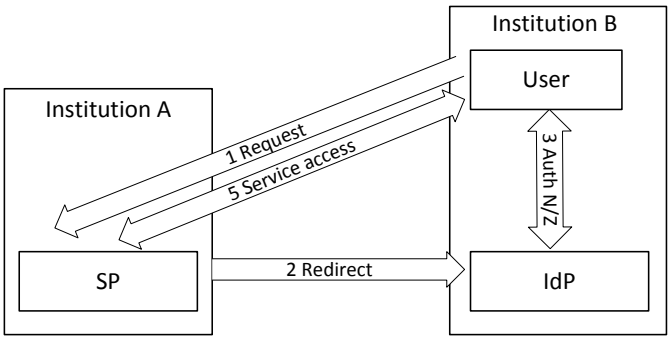
În cadrul RȘEN în Mai 2014 a fost inițiat un proiect pilot de creare a *Resurselor Federative Naționale* cu o ulterioara extindere către resursele și serviciile din cadrul *eduGain*.

În acest scop au fost definiți pași, cu implicarea instituțiilor din cadrul rețelei naționale științifice, care prevăd:

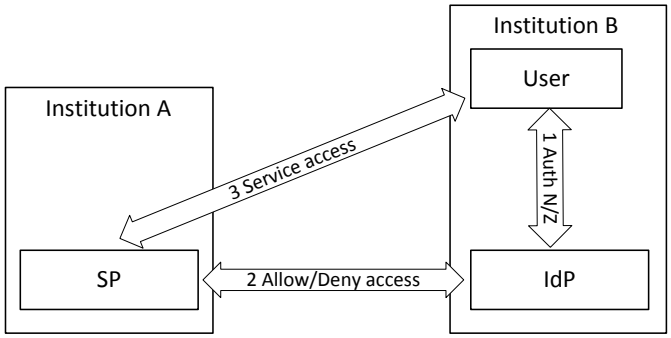
- Elaborarea și semnarea unui acord de colaborare și politicelor de prestare a serviciilor.

  În acord sunt stipulate contribuțiile fiecărui membru pentru dezvoltarea *Resurselor Federative Naționale*, beneficiile membrilor acordului de colaborare. Politicele descriu procesul de prestare a serviciilor în cadrul

Resurselor Federative Naționale și procesul de management al identității în cadrul acesteia.



a)



b)

Fig. 6 Căi de acces a serviciilor federative.

- Implementarea și testarea unei AAI în cadrul rețelei naționale științifice.

Acest compartiment constă dintr-un șir de activități destinate pentru elaborarea, implementarea, depanarea și validarea unei structuri fiabile AAI în cadrul *Resurselor Federative Naționale*. Implementarea va avea loc în două etape: o realizare locală care va fi constituită dintr-un serviciu și un element IdM, și una la nivel al rețelei naționale științifice. Fiecare din aceste implementări are ca scop testarea procesului de funcționare al IdM la generarea metadatelor, testarea și formarea setului minim de date necesare pentru formarea accesului către serviciile intra-federație sau inter-federative. Ca rezultat final al acestor activități vor fi documentele tehnice care vor specifica cerințele către componentele IdM.

- Aderarea la resursele internaționale, propunând un set de servicii competitive din cadrul *eduGain*.

Procesul de implementare a serviciilor federative la nivel național este unul de lungă durată, unde un interval mare de timp este acordat scrierii și aprobării documentelor de diferită natură, cum ar fi acorduri sau documente tehnice, care sunt aprobate de toate instituțiile participante[5]. Serviciile partajate depind de componenta IdP, unde schimbul de date între membrii atât a federației cât și în afara ei, este un proces important de acces la rețele și aplicații și asigură circulația informației senzitive între rețele, deci utilizarea aplicațiilor pentru schimb de date prevede analiza preventivă a aplicațiilor și protocoalelor ce urmează a fi folosite.

V. Rezultate

În implementarea preventivă al AAI au fost utilizate mașini virtuale din cadrul NOC RENAM și DI ASEM. Din mulțimea de aplicații care realizează protocolul SAML a fost selectat pachetul *simpleSAMLphp*, instalat în instanțe IdP și SP. Aceste instanțe au fost cu succes conectate la LDAP(IdP), Moodle și Joomla(SP). În baza pachetului *simpleSAMLphp* a fost implementat *SP initiated login* (fig. 6a), între IdP și Joomla cu pachete SP din surse terțe, și IdP *initiated login* (fig. 6b) între IdP și Moodle cu modulele integrate.

Bibliografie

[1] www.geant.net, "Federating GN3 Services – Géant"
[2] www.geant.net, "Identity Federations"
[3] BOGATENCOV P., POCOTILENCO V. Implementation of national IdP Management Systems for Access to Resources of European R&E E-Infrastructures. "Networking în Education and Research", Proceedings of the 11th RoEduNet IEEE International Conference, Sinaia, Romania, January 17-19, 2013, 96-100. ISSN-L 2068-1038.
[4] Andreas Åkre Solberg, Roland Hedberg "GÉANT Federation", TNC2012.
[5] Brook Schofield, "Introduction to Identity Federations" EUROCamp2012
[6] http://docs.oasis-open.org "Security Assertion Markup Language (SAML) V2.0 Technical Overview"