A Dynamic and Flexible Security Framework

Coordonatori:
Prof. Dr.Ing. Nicolae Tapus
Dr. Iosif Legrand
As.Ing. Ramiro Voicu

MonALISA

Sistem distribuit de colectare a informatiilor de monitorizare (resurse,trafic) bazat pe servicii (JAVA/JINI, WSDL/SOAP).

Serviciile Monalisa utilizeaza mecanisme dinamice de inregistrare/cautare in servicii specializate (Lookup Services).

Mecanismele de securitate

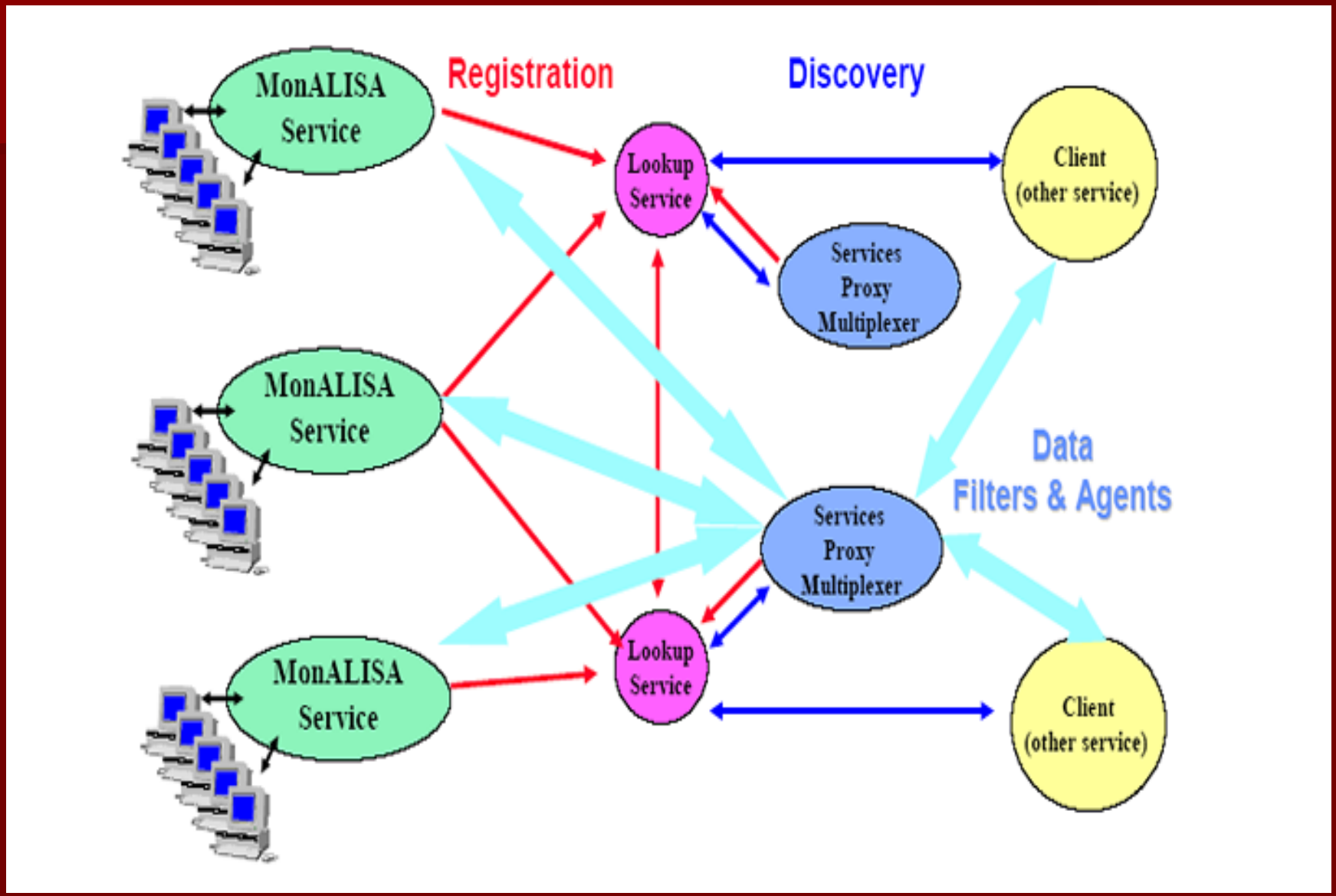
...trebuie sa permita si sa asigure:

- Autentificare
- Autorizare
- Confidentialitatea comunicatiei
- Integritatea datelor

- Autentificare si autorizare:
  - autentificarea este procesul prin care se utilizatorul isi demonstreaza identitatea in cadrul unui sistem;
  - Autorizarea estre procesul prin care se determina (pe baza unor politici de securitate) ce permisiuni are un utilizator in cadrul unui sistem.
- Confidentialitate
  - Se asigura prin criptarea (simetrica) datelor;
  - Pentru a transfera cheile secrete se utilizeaza o infrastructura PKI;
- Integritatea datelor
  - Asigura ca datele transmise nu sunt alterate
  - Se utilizeaza algoritmi de generare de rezumate a datelor (message digest) (ex.MD5, SHA) care se calculeaza la ambele capete ale comunicatiei.

- Platforma Java pune la dispozitie extensii prin care se asigura toate aceste cerinte:
  - JavaTM Authentication and Authorization Service API (JAAS)
  - Java Cryptographic Extension (JCE)
  - JavaTM Secure Socket Extension (JSSE)
  - Java Naming and Directory Interface (JNDI)

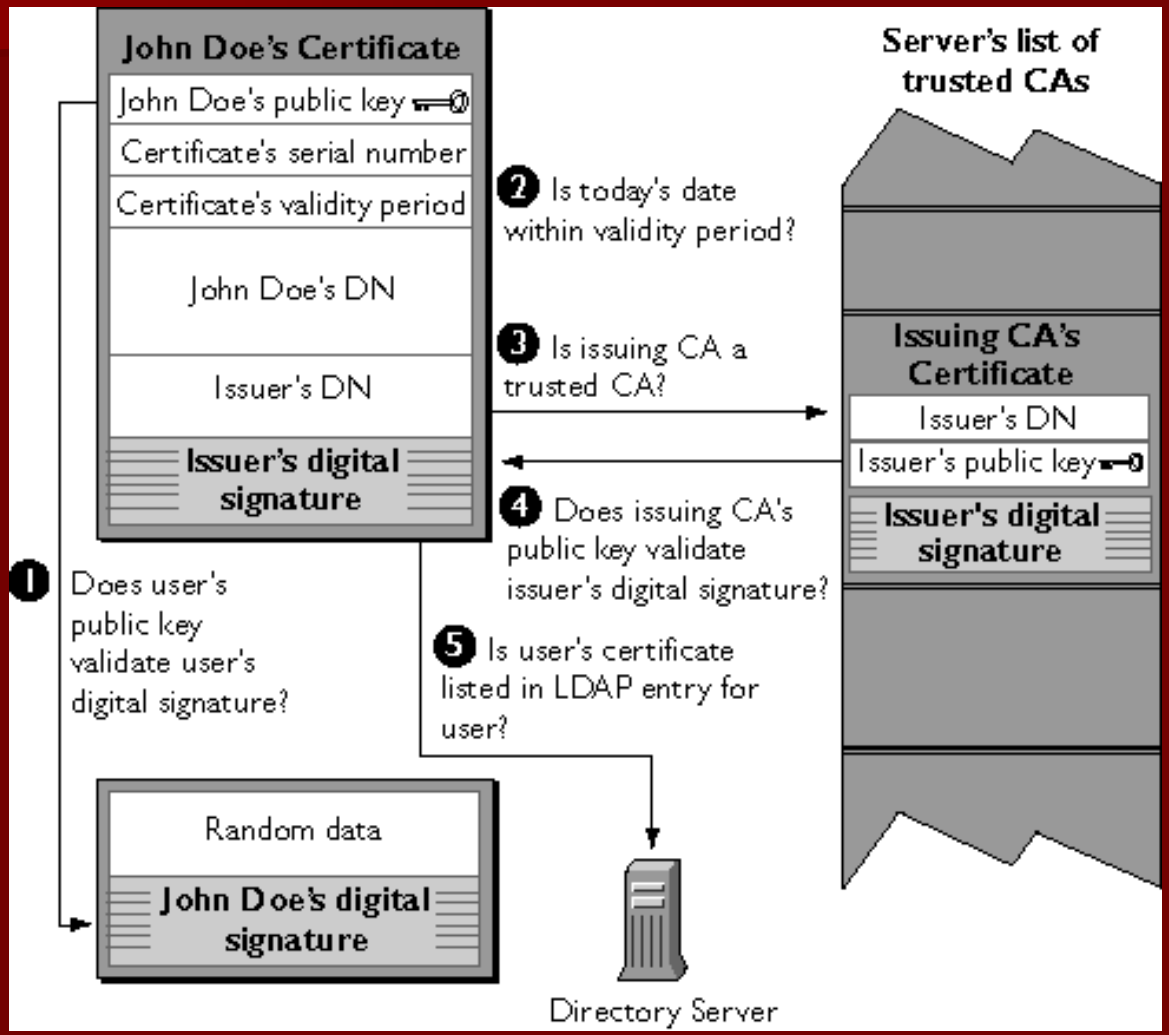
Arhitectura MonALISA



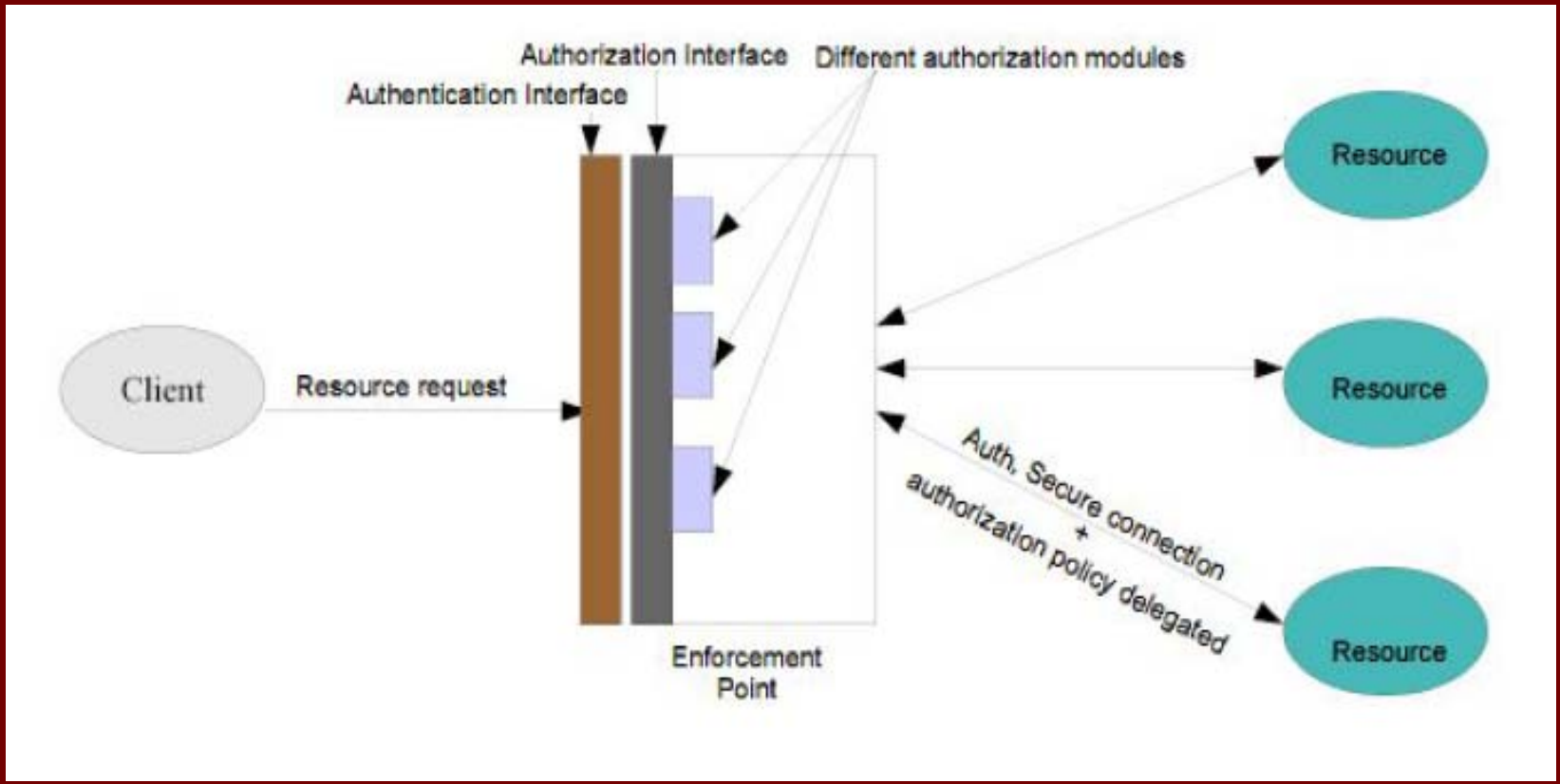
Cerinte de securitate

- Posibilitatea limitarii accesului la serviciile MonaALISA
- Autentificare si autorizare flexibila
- Confidentialitatea si integritatea datelor

SSL Authentication Protocol (SAP)



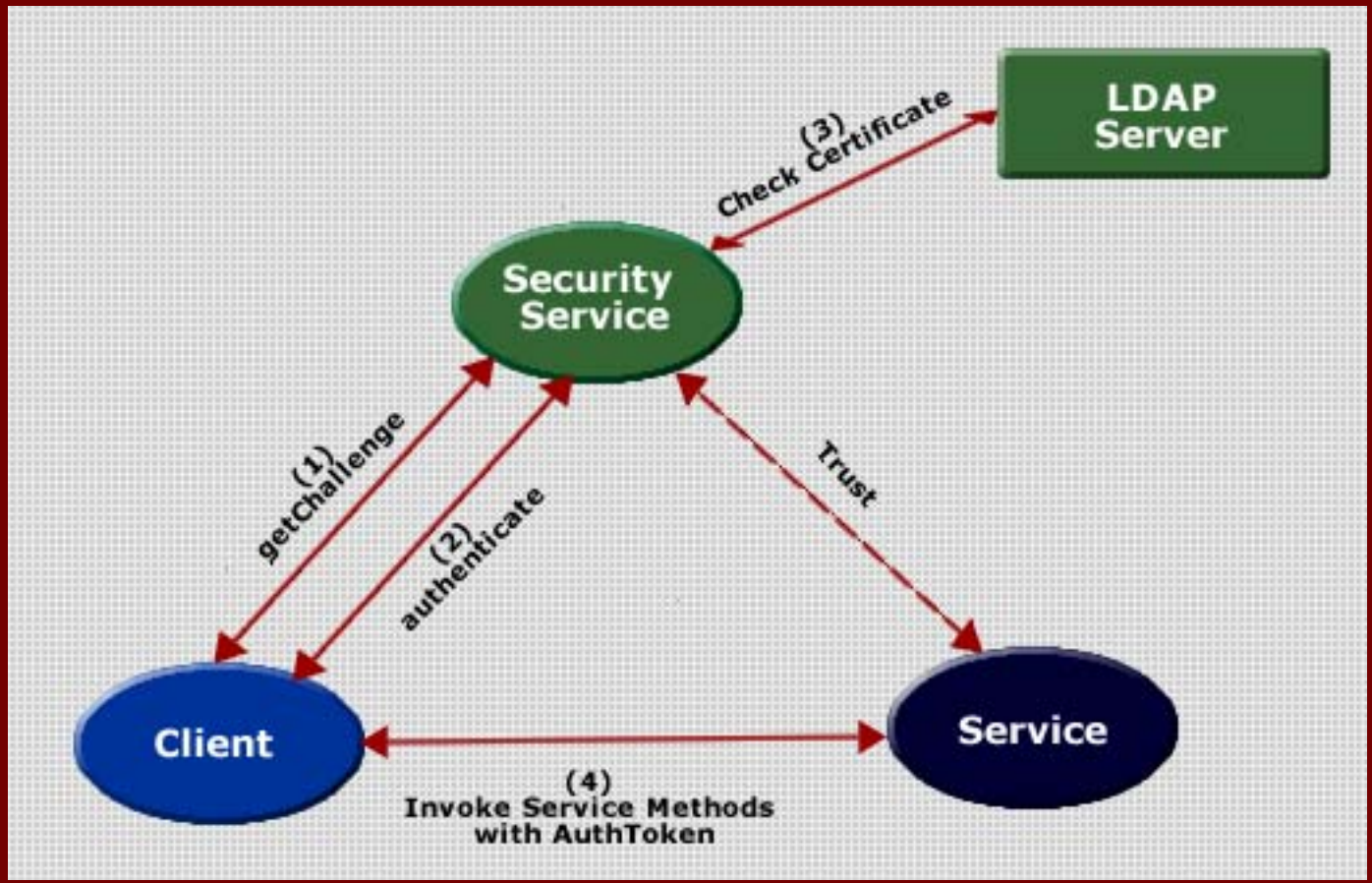
Solutie de autorizare PDP/PEP distribuit



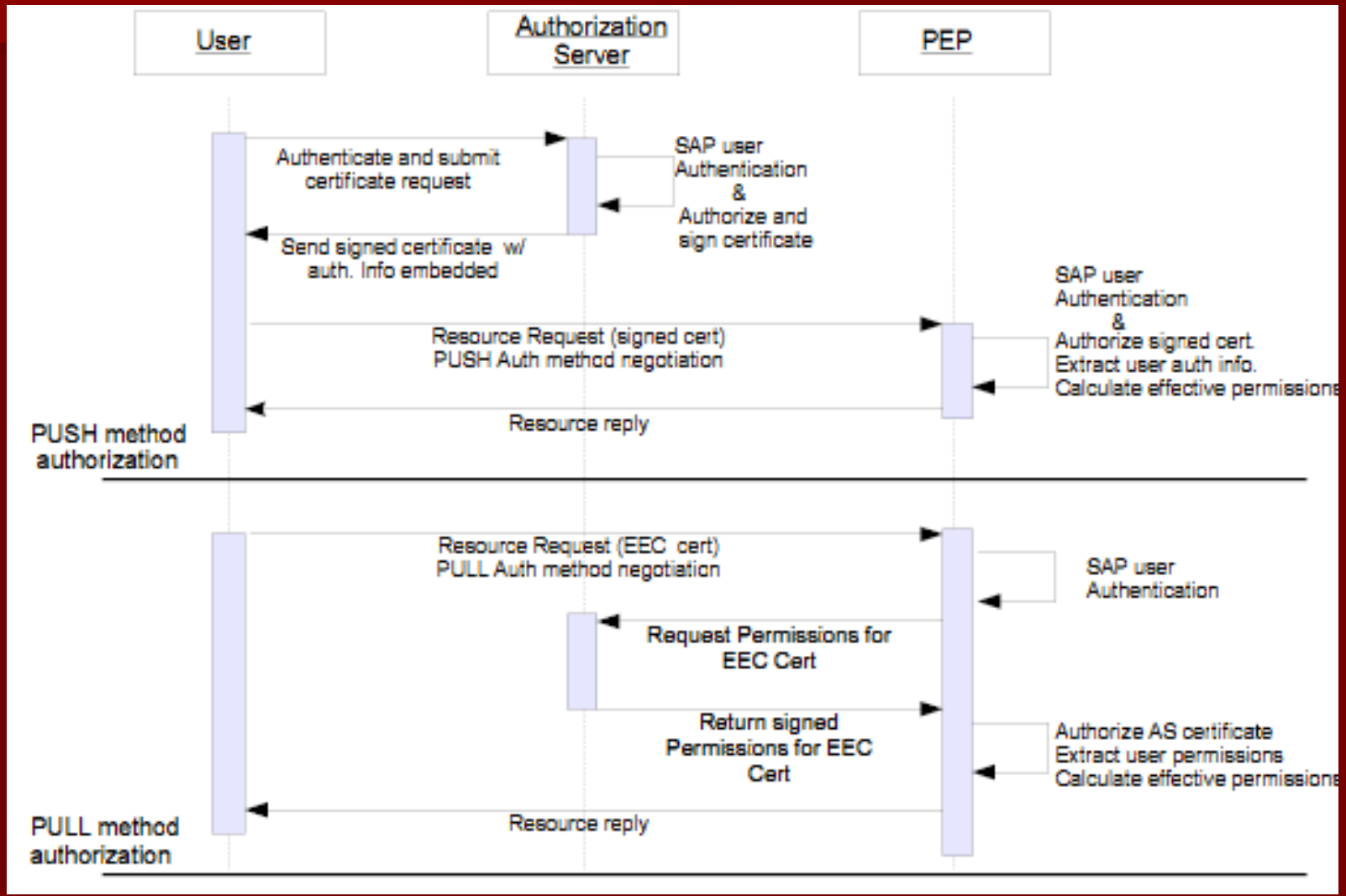
Diferite modele de autorizare

- Push model
- Pull model
- Self model (fara un tert serviciu de autorizare)
- Anonymous

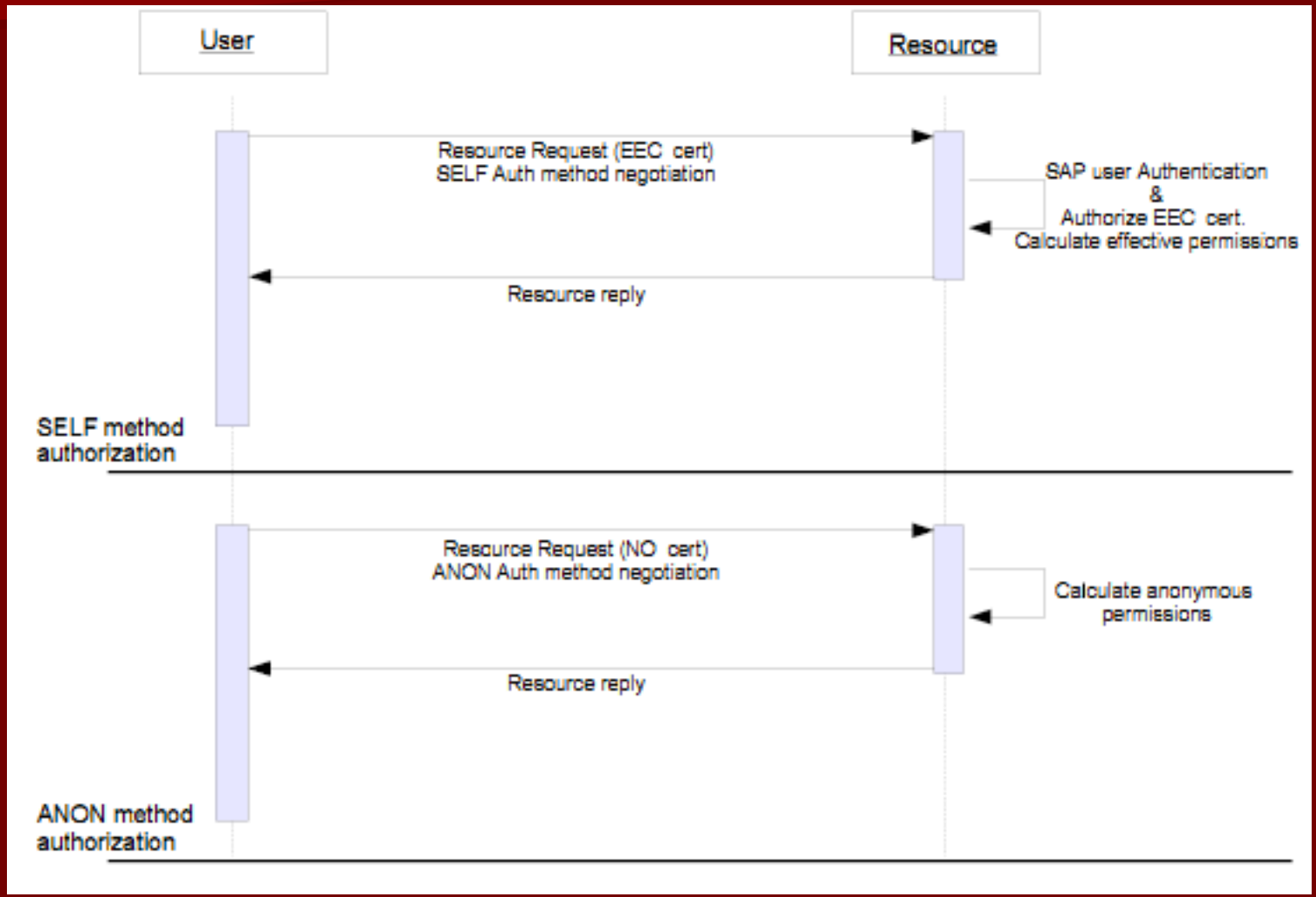
Push Model


LDAP Server
(3) Check Certificate
Security Service
(1) getChallenge
(2) authenticate
Trust
Client
Service
(4) Invoke Service Methods with AuthToken

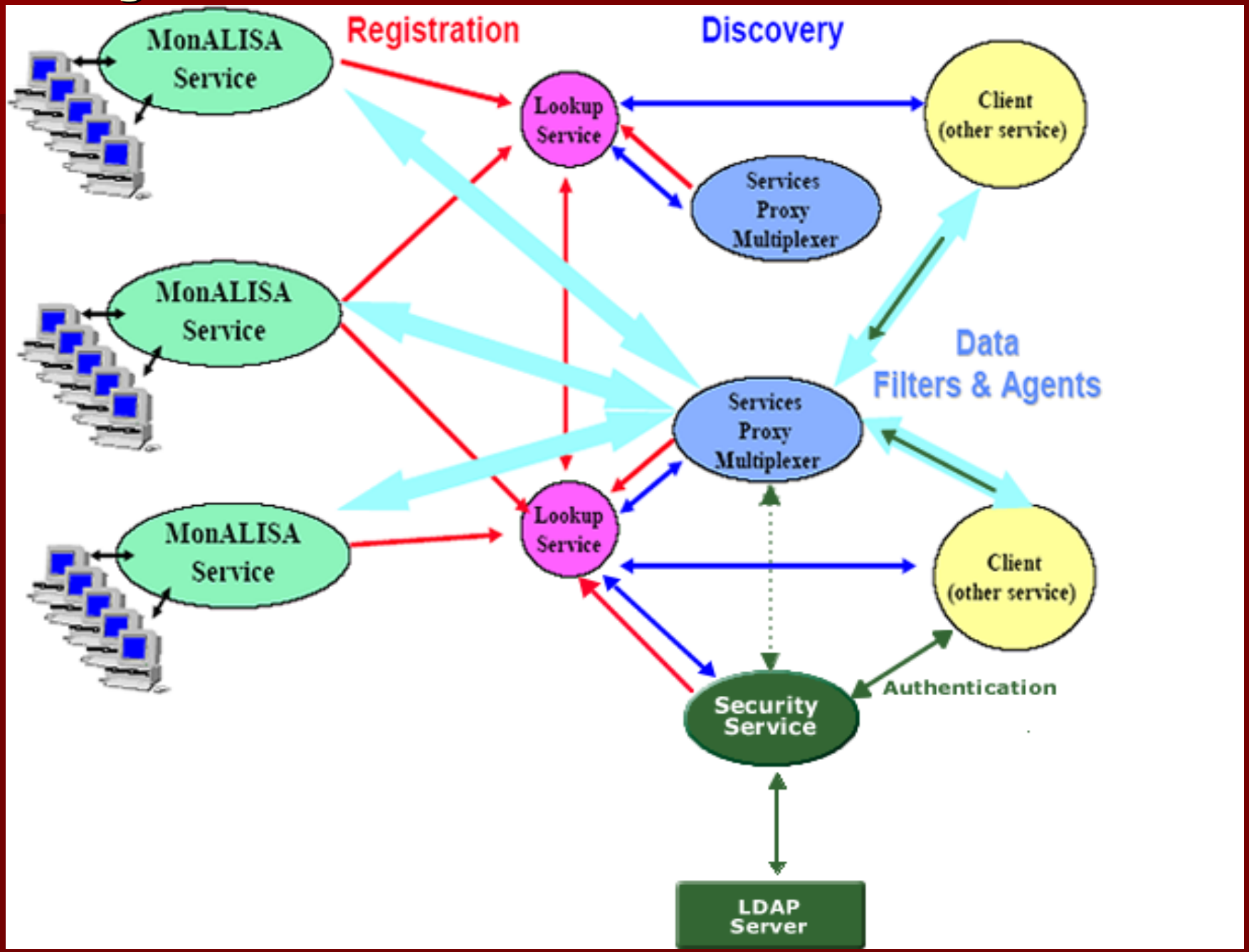
Module de autorizare (push, pull)



Module de autorizare (self, anon.)



Integrarea acestui mecanism de autentificare in Monali



Avantajele acestei scheme de autentificare …

- Elimina necesitatea ca etapele de autentificare si autorizare sa se execute de fiecare data cand un client doreste sa utilizeze un serviciu (single sign on);
- Delegarea de catre serviciu a etapei de autorizare catre un gatekeeper
- Module de autorizare de tip plug-in pot fi dezvoltate ulterior.

Bibliografie

- MonALISA
  http://monalisa.cacr.caltech.edu/
- *Security*, Accounting, and Assurance chapter in
  The GRID: Blueprint for a New Computing Infrastructure
  B. Clifford Neuman
- *A Community Authorization Service for Group Collaboration.*
  L. Pearlman, V. Welch, I. Foster, C. Kesselman, S. Tuecke.
- Security for Grid Services. V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, S. Tuecke.