

# Tema de casă #3 – Implementarea unui serviciu securizat de gestiune a documentelor

**Responsabil de temă:** Ciprian Dobre (ciprian.dobre@cs.pub.ro)

**Data publicării:** 18.11.2008

**Data ultimei modificări a enunțului:** 18.11.2008

**Termenul de predare:** 08.12.2008

## Obiective

După realizarea acestei teme de casă studentul va fi capabil să:

- Realizeze o aplicație bazată pe folosirea unor soluții de securitate în Java.
- Gestioneze eficient structuri de date folosite în rezolvarea unor probleme similare.
- Realizeze programe ce folosesc transmisii sigure de mesaje, autentificare, criptare.

Cunoștințele necesare rezolvării acestei teme de casă:

- Programare folosind Java
- Cunoștințe privind mecanismele de securitate puse la dispoziție de Java pentru securitate.
- Detaliile de folosire ale claselor din pachetele Java pentru securitate prezentate în cadrul laboratorului.

## Enunțul problemei

Se cere implementarea unui sistem de gestiune a documentelor. Sistemul este format din aplicații client, o aplicație server și un Serviciu de Autorizare.

Presupunem că există o instituție ce pune la dispoziția angajaților săi un sistem de gestiune a documentelor. Compania este formată din mai multe departamente (Contabilitate, Resurse Umane, IT, etc.).

În cadrul sistemului se consideră că un utilizator este identificat unic prin intermediul unui certificat X.509 eliberat de Autoritatea de Certificare din cadrul companiei și care are numele unic (DN) de forma :

CN=IonPopescu, OU=Accounting, O=MyCompany, L=Bucharest, ST=Romania, C=RO

Presupunem că există un server central de gestiune a documentelor ce deservește angajații companiei. Aplicația server acceptă doar conexiuni SSL și utilizează un certificat propriu semnat de CA-ul companiei. Pentru început clientul se conectează la unul dintre servere folosind o conexiune SSL cu autentificare bidirecțională (atât serverul cât și clientul își trimit certificatele). Handshake-ul reușește numai dacă certificatul prezentat de client este semnat de către CA. În cadrul sistemului clienții sunt identificați prin numele câmpului CN din certificatul prezentat.

În sistem clienții au rolul de a citi documente și de a încărca pe server noi documente. În aplicația server pentru fiecare document veți păstra o informație referitoare la identitatea proprietarului, a clientului ce a uploadat respectivul document, și la identitatea departamentului de care acesta aparține. Pentru ca această informație să nu se piardă nici după repornirea serverului veți folosi un fișier. În acest fișier veți scrie mapări (nume\_fișier, identitate\_proprietar, departament), fișierul fiind întotdeauna ținut criptat pentru a face imposibilă divulgarea informației (metoda de criptare o alegeți voi, însă trebuie să o amintiți în fișierul Readme). Pentru departament se va folosi de câmpul OU ce desemnează departamentul din care face parte utilizatorul proprietar. La pornirea aplicației server veți citi conținutul fișierului în memorie.

Un client va încerca inițial stabilirea conexiunii cu serverul de gestiune a documentelor. Dacă conexiunea reușește, acesta va intra într-un mod interactiv în care poate primi comenzi din partea utilizatorului (implementați primirea de comenzi fie din consola text, fie o interfață grafică minimală). Comenzile posibile sunt: list, download, upload. Comanda list va întoarce lista de fișiere existente în aplicația server. Comanda upload va avea ca rezultat încărcarea unui fișier pe server. Comanda download are rolul de a indica dorința începerii unui download (primește ca parametru numele unui fișier). Pentru download aplicația server va „autoriza” mai întâi clientul. Aplicația server va stabili o conexiune SSL cu Serviciul de Autorizare (serviciul central) și pe această conexiune aplicația interoghează Serviciul pentru a afla dacă DN-ul clientului este autorizat sau nu să downloadeze documentul aparținând unui anumit departament. Fiecare departament al companiei are atașată o anumită prioritate pe baza căreia un utilizator are acces sau nu pe un server de documente. Un utilizator aparținând unui anumit departament nu are acces decât la fișierele departamentelor având o prioritate mai mică sau egală. De exemplu departamentul Management are o prioritate maximă, aceasta însemnând că un utilizator din acest departament va avea acces la documentele tuturor celorlalți utilizatori. Pe baza politicii pe care o veți defini voi Serviciul de Autorizare va trimite serverului un răspuns prin care va informa dacă respectivul utilizator are drept sau nu de download.

Dacă răspunsul este favorabil, comanda download va avea ca rezultat transferarea fișierului și salvarea acestuia local, la client, într-un director numit „download”.

Tot aplicația server va avea și rolul de a monitoriza fișierele curent uploadate. Dacă aplicația server întâlnește de exemplu „bomba” sau „greva” în numele unui fișier (lista de cuvinte cheie o definiți voi) atunci va „bloca” utilizatorul respectiv. Pentru aceasta numele de utilizator va fi trimis Serviciului de Autorizare care îl va scrie într-un fișier de utilizatori "banned" într-o formă încriptată cu formatul "nume time". "Time" înseamnă momentul de timp când a fost scrisă respectiva intrare. Un utilizator blocat va rămâne blocat pentru un timp maxim prestabilit de voi, timp în care el nu are voie să mai downloadeze de la server nici un document (în pasul de verificare a departamentului veți întoarce răspuns negativ dacă respectivul client este în lista de banned). Dacă Serviciul de Autorizare este repornit el va reciti datele despre utilizatorii blocați din respectivul fișier.

## **Precizări legate de implementarea temei**

Aplicația va fi implementată în Java. Pentru implementare folosiți JSSE (<http://www.panix.com/~mito/articles/#jsse>) și JCE (<http://java.sun.com/products/jce/>). În fișierul Readme veți detalia aspecte legate de implementare, veți explica deciziile pe care le luați asupra algoritmilor de criptare folosiți.