CSC436 Secure Programming

Project 1

(due by midnight on Wedesday, October12)

Project 1 must be submitted electronically, using the Blackboard Digital Dropbox facility of the course website. Your submission must include 3 files:

(a) Source code
(b) Class files
(c) 1-2 page description of the program as ASCI text documents, MS Word documents, or a PDF file.

Please do not zip files.

Write two programs in Java called Client and Server. The Server program acts as an access controller to a sensitive system resource by validating every attempt to use the resource. The Server maintains a list of authorized users which can access the resource.

The Client generates and sends a request to the Server for using the resource. The request is written in a file on the system disc, which contains:

a) A digital signature for the system date, signed with the user private key.

b) A digital certificate of the user, containing the name of the user and his public key. The certificate is self-signed.

The server opens the file and grants access to the resource if and only if:

a) The digital signature is verified with the public key from the certificate.
b) The user name is in the list of authorized users.

The Server outputs a message “Access granted” or “Access denied” based on the credentials of the Client.