Systèmes distribués - Master 2ème année

TP à rendre pour le 01/12/08

L'idée générale de ce TP est d'utiliser plusieurs des technologies vues en cours de Systèmes Distribués. Ne cherchez donc pas une logique quelconque à l'architecture générale car il serait difficile de la justifier dans un contexte réel. Le but est d'avoir un serveur Java qui délivre des certificats X509 à deux clients, disposant de clés, pour permettre à ces derniers d'établir une connexion **sécurisée** et **authentifiée**. Cet échange ne se fera pas directement mais plutôt à travers un relais qui permettra la communication entre C et Java.

Le serveur Java

Le serveur Java est, à la fois, un publisher et un receiver JMS. Il annonce sur un topic, déclaré à travers jndi, qu'il se propose comme serveur de certificats. Pour cela, il envoie régulièrement des messages sur le topic annonçant qu'il est prêt à délivrer des certificats. Il donne dans ces messages les références nécessaires à l'accès à sa queue.

Le serveur dispose également d'une queue sur laquelle il reçoit les demandes de certificats : soit pour donner son certificat en tant que autorité de certification soit pour créer un nouveau certificat à partir d'une clé. Dans le cas d'une création, la demande de certificat doit contenir une clé. le serveur enregistre alors la clé dans un fichier et génère le certificat correspondant en lançant la commande shell (voir la classe Runtime) de génération d'un certificat. Il envoie ensuite le certificat demandé à son client.

Les clients

Les clients sont écrits en C/C++. Le but est de leur permettre d'établir une communication sécurisée et authentifiée. A l'origine, chaque client dispose d'une clé enregistrée dans un fichier qui sera créée à la main à partir de la commande openssl. Le client demande au relais un certificat, en lui fournissant sa clé. En retour il reçoit un certificat qu'il enregistre dans un fichier. Il demande également le certificat de l'autorité de certification. Un fois les trois éléments mis en place, le client établit une connexion sécurisée avec l'autre client et échange un message de bienvenue.

Les relais

Les relais sont écrits en Java. Ils utilisent Corba et JMS. Un relais est en attente d'une demande de certificat de la part du client. Le relais peut recevoir deux types de requêtes : des requêtes de certificat racine et des requêtes de nouveau certificat. Lorsqu'il reçoit, une telle requête le relais se met en attente sur le topic du serveur d'un message annonçant que le serveur délivre des certificats. Une fois le message reçu, il accède à la queue donnée dans le message pour envoyer sa requête et obtenir soit le certificat demandé. Avant de retourner un certificat au client le relay doit afficher les informations liées à ce certificat : le DN du propriétaire, le DN de l'autorité et la date de validité du certificat.

Indication complémentaires

Pour la gestion des certificats en Java, il est recommandé d'utiliser les classes Certificate, X509Certificate et certificateFactory : elles contiennent toutes les méthodes nécessaires à la manipulation de vos certificats. Leur utilisation peut se faire à partir de ce qui a été vu dans le cours sur la sécurité dans Java.

Ce TP peut être rendu par binômes. Vous ferez une démonstration de l'exécution de votre application et vous rédigerez une documentation expliquant vos choix de réalisation et de développement.