# Laboration 6 – PKI med JSSE

## Innehåll

Att med hjälp av SSLSockets implementera en krypterad förbindelse.

## Uppgifter

Skapa ett certifikat med *keytool*. Utgå sedan från filen Server.java och Certifikat.java och skapa en server som väntar på en inkommande krypterad anslutning. Det räcker med att servern skriver ”HelloWorld” eller likande. När anslutningen väl är upprättad kan ni ändå lägga till vilken javakod som helst. Vad ska ni ansluta med som klient? Godtycklig webläsare t ex Internet Explorer eller Firefox! Ett tips är att prova dem båda för säkerhets skull. Om ni får problem kan det vara en god idé att titta under säkerhetsinställningarna i webläsaren samt även att prova att ansluta från en annan dator. Vid redovisningen är det viktigare att ni kan förklara PKI-modellen än detaljer i koden (då man kan använda samma kod om igen för godtyckligt projekt där man behöver kryptering).

## Extrauppgift:

Ni ska i java skriva en terminalbaserad epostklient mot CSC:s IMAP-server *mail1.nada.kth.se*. Den ska presentera en lista på era mail och sedan ska ni kunna markera ett mail och ladda ned det för visning. Ni får ej använda *javamail* till denna uppgift utan tanken är att öva på krypteringsklasserna. Ej heller s k *system properties*. Tänk på att det finns risk att programmet tankar ner samtliga era mail från servern! Dessutom kan det vara så att ditt konto har automatiskt vidarebefordring av mail, d v s alla dina mail till @csc.kth.se går till @kth.se. I s f måste du ändra detta då mailboxen annars kommer vara ständigt tom. Detta kan bl a ändras med UNIX-kommandot *chpobox*. För att bli godkänd på extrauppgiften måste man även ha gjort grunduppgiften.