

Medical Records & Secure Connections:  
Projektarbete i kursen Datorsäkerhet (EIT060)  
EIT, Institutionen för Elektro och  
Informationsteknik, Lunds Tekniska Högskola  
Martin Hell

Adam Hansson Lyrén, C11 (dic11aha@student.lu.se)  
Johan Bäversjö, C11 (dic11jba@student.lu.se)  
Mergim Rama, C11 (dic11mra@student.lu.se)  
Sven Elfgrén, C11 (dic11sel@student.lu.se)

26 februari 2013



**LUNDS**  
**UNIVERSITET**  
Lunds Tekniska Högskola

# Innehåll

<b>1</b>	<b>Introduktion</b>	<b>2</b>
<b>2</b>	<b>Bakgrund</b>	<b>2</b>
2.1	Socialstyrelsen . . . . .	2
2.2	Läkare . . . . .	2
2.3	Sköterska . . . . .	2
2.4	Patienter . . . . .	3
<b>3</b>	<b>SSL/ TSL</b>	<b>3</b>
<b>4</b>	<b>Certifikat</b>	<b>3</b>
<b>5</b>	<b>Säkerhetsutvärdering</b>	<b>3</b>
<b>6</b>	<b>Referenser</b>	<b>3</b>

# 1 Introduktion

Projektet handlar till stor del om hur man kan upprätta en säker och krypterad anslutning mellan klient och server. För att kunna upprätta denna anslutning kommer vi använda oss av Secure Socket Layer (SSL) protokollet. Djupare teknisk beskrivning av SSL kommer senare i rapporten. Detta projekt kräver att man från grund skapar en verklig produkt som kan användas av verkliga organ. När vi använder oss av SSL protokollet kommer vi även använda oss av Java Secure Socket Extension (JSSE). Efter att ha skrivit klart programmet ska det säkerhetsutvärderas. Denna säkerhetsutvärdering täcker alla olika attacker som kan uppstå mot systemet och vilka attacker systemet kan skydda sig mot.

# 2 Bakgrund

Problemet som projektet grundar sig på är att skapa säkra medicinska journaler för ett sjukhus. Med säkra journaler menas i detta fall journaler som är sekretessbelagda så att inte vem som helst kan ha tillgång till dem, det vill säga att patienternas integritet skyddas. Eftersom systemet är en produkt framtagen för riktig användning måste det begränsas så att olika grupper på sjukhuset har olika behörigheter till journalerna. Personer som inte har någon behörighet kommer aldrig att kunna nå journalerna. De olika grupper som ska finnas med är:

1. Socialstyrelsen
2. Läkare
3. Sköterska
4. Patienter

## 2.1 Socialstyrelsen

Socialstyrelsen är det organ som bestämmer, det vill säga de har befogenheter till att kunna ta bort samt lägga till journaler.

## 2.2 Läkare

Läkaren kan däremot skriva och läsa färdiga journaler, förutsatt att han är den som tar hand om patienten. Han kan också läsa journaler som finns på hans avdelning. Om patienten inte har någon journal har läkaren befogenheten till att skapa journalen. Kravet är då att läkaren själv är den som behandlar patienten.

## 2.3 Sköterska

Sköterskans rättigheter är att hon kan läsa och skriva till journalerna som hon är skriven på och att läsa alla journaler från hennes avdelning.

## **2.4 Patienter**

Patienterna är berättigade till att läsa endast sina egna journaler vilket är en självklarhet. För att kunna spara allt som händer på journalerna ska en logg föras som visar vem som gjort vad i journalen samt vid vilken tidpunkt det hände.

## **3 SSL/ TSL**

Teknisk beskrivning av SSL/ TLS och vi implementerar detta i vårt system.

## **4 Certifikat**

Teknisk beskrivning av certifikat och vi använder det i vårt system.

## **5 Säkerhetsutvärdering**

Säkerhetsutvärdering av systemet.

## **6 Referenser**

Referenser till olika tekniska begrepp som kommer att nämnas.