## Attackmetoder

MITM  
Genom att klient/server att först autentiserar sig mot varandra undviks MITM-attacker.  
Eftersom den privata nyckeln krävs för att dekryptera handskaket blir eventuell uppsnappad information värdelös.

Spoofing  
Det finns ingen möjlighet att skapa en falsk server eftersom denna saknar det (enda) tillförlitliga certifikatet för klienten. Servern misslyckas med att autentisera sig och ingen känslig information läcker ut.

Avlyssnad kommunikation  
Oanvändbar utan den hemliga nyckeln.

Falska certifikat  
Servern kontrollerar truststore och nekar anslutning.  
  
Lösenordspolicy  
Undgå dictionary- och rainbowattacker genom att vara långt, bestå av varierande teckentyper och inte bestå av ord. Byta lösenord på regelbunden basis, logga misslyckade inloggningsförsök.  
  
Mänskliga faktorer  
Se till att vanliga användare inte kan ändra på säkerhetspolicy/lägga till certifikat. Ha minimumkrav för egenskapade lösenord.

Attack mot journaldatabasen?  
Ladda ned och sprida journaler utanför den säkra uppkopplingen?  
Elektromagnetisk avläsning av knapptryckningar?  
Attacker mot en enskild mot keystore för att skapa nytt certifikat?  
Överbelasta servern, DDOS eller motsvarande?  
Möjlighet att förneka att man utfört en viss handling i en journal?

Frågeställningar  
Vem får skapa certifikat/ändra accessnivåer, kan detta missbrukas?  
Journal som tas bort av misstag eller av illvilja, kan den återställas?   
Finns det någon möjlighet till SQL-injektion?