inera
LANDSTING OCH REGIONER
I SAMVERKAN FÖR E-HÄLSA

Teknisk beskrivning SITHS Root CA

Informationsunderlag för nödvändiga förberedelser för system som använder SITHS certifikat

Revisionshistorik		
Version	Författare	Kommentar
1.0	Carl Önne	Upprättande av dokumentet
1.1	Carl Önne	Justering av beteckningar
1.2	Christoffer Johansson	Tillägg till instruktioner för Installation av Root CA v1 på klientdator och Appendix A
2.0	Christoffer Johansson	Total omstrukturering av dokumentet samt namnbyte
2.1	Carl Önne	Korrekturläst
2.2	Christoffer Johansson	Rättning av länkar, tillägg av information om Crossborder och gamla Testmiljöerna samt tydliggörande av CNAME för sithsocsp.trust.telia.com
2.3	Christoffer Johansson	Borttagning av länkar till undersidor på www.inera.se
2.4	Christoffer Johansson	Rättning av IP-adresser för sökvägar till spärrinformation via LDAP över Sjunet för gamla CA's
2.5	Christoffer Johansson	Rättning av IP-adresser för gamla PKI:n
3.0	Christoffer Johansson	Byte av IP-adresser efter flytt av CRL- och AIA-server på Sjunet från Inera till Basefarm, samt flytt till Ineras nya dokumentmall.
3.1	Christoffer Johansson	Uppdatering av IP-adresser efter flytt av och uppdelning mellan produktion och preproduktion för SAMTLIGA CRL- och AIA-servrar till från Basefarm till Telia, 5 september 2016 kl 13:00

Innehållsförteckning

1. SITHS Root CA

Detta dokument beskriver de **grundläggande** tekniska förutsättningarna för klienter och system som använder sig av SITHS certifikat vid identifikation.

Detta dokument vänder sig till systemförvaltare, systemtekniker och systemleverantörer.

Dokumentet är inte avsett att beskriva någon bakgrund till hur certifikat och PKI fungerar. Inte heller gör det anspråk att vara helt komplett gällande hur respektive system ska hanteras/ anpassas klara av SITHS Root CA. Det ska ses som informationsmaterial som pekar på behoven av förberedelser i respektive system.

För mer teknisk information om hur en trust store och validering av certifikat fungerar i Microsoft, finns en artikel här: http://technet.microsoft.com/en-us/library/cc778623(v=WS.10).aspx.

1.1 Begrepp

Begrepp	Förklaring
SITHS Root CA v1	Benämns hädanefter v1 och syftar till den PKI som är aktiv inom tjänsten SITHS sedan den 30 januari 2013
SITHS Root CA v3	Benämns hädanefter v3 och syftar till den PKI som håller på att avvecklas, men är giltigt fram till den 28 november 2015

1.2 Skiss SITHS PKI

Nedan visas en skiss på hur den nuvarande och den gamla PKI:n kan jämföras.

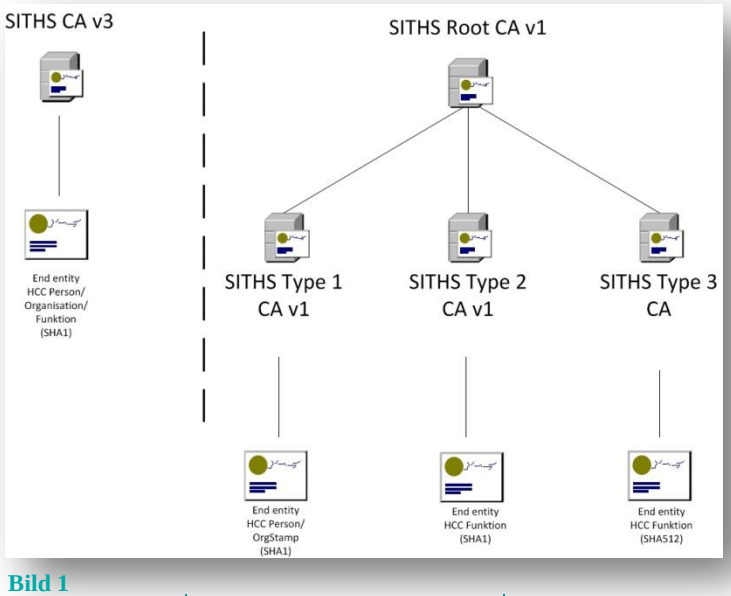


Bild 1

1.3 Nuvarande PKI

1.3.1 SITHS Root CA v1

Nuvarande PKI bygger på en Certifikatkedja (Chain of trust) som kort innebär att en Root CA med lång giltighetstid (2032-03-29) ställer ut certifikat till mellanliggande certifikatservrar, vilka i sin tur ställer ut certifikat för person och funktion. För v1 finns i dagsläget 3 mellanliggande servrar:

- SITHS Type 1 CA v1 – HCC Person
- SITHS Type 2 CA v1 – HCC Funktion, #PKCS12, SHA-1
- SITHS Type 3 CA v1 – HCC Funktion, #PKCS10, SHA-512

För att applikationer och system ska kunna verifiera de certifikat som produceras måste följande vara på plats:

1. Rotcertifikatet för v1 måste finnas med i aktuell trust store både på klienter och på servrar.
2. Klienter och Servrar måste klara av att bygga en ”Chain of trust” till rotcertifikatet, via ett mellanliggande certifikat.
3. System måste vara förberedda på att hantera nya nyckelstorlekar, från 1024 till 4096 och 2048 (RSA-nycklar).
4. Samtidigt som man ser över certifikatsanvändningen i systemen, är det bra att inventera vilka system som har- respektive inte har kompatibilitet med signeringsalgoritmen SHA512[1]. Detta då man i framtiden avser nyttja HCC Funktion från den nya Type 3 CA:n för ökad säkerhet.

1.3.2 SITHS Crossborder

Om ni har behov av att kunna hantera personal utan svenska personnummer i er organisation (Crossborder), finns också en PKI som heter SITHS Crossborder CA[2]. Detta läses in manuellt enligt någon av checklistorna under rubrik 3 & 4 nedan.

[1] Microsoft XP har stöd för SHA512 först i SP3, se t.ex. http://blogs.technet.com/b/pki/archive/2010/09/30/sha2-and-windows.aspx

[2] Personer utan personnummer, kan inte få ett Telia eID, vilket är grunden för SITHS. Dessa får istället ett s.k. Crossborder-certifikat som är ett tredje PKI, ej inritat på bilden ovan.

1.4 PKI under avveckling

Giltighetstiden för SITHS CA v3 upphör den 28 november 2015. Dessutom har hotbilden på Internet ökat, vilket ställer hårdare krav på certifikat-utfärdare gällande bl.a. utfärdarrutiner och nyckellängder. Detta har resulterat i att man den 30 januari 2013 införde en ny CA struktur inom SITHS. Eftersom förändringen rent infrastrukturellt var ganska omfattande valde man att starta om versionshistoriken för SITHS och döpa den nya till SITHS Root CA version 1 (tidigare kallad v5)[3].

Den utgående SITHS CA v3 är en PKI vars rotcertifikat är giltigt fram till 2015-11-28. Men redan i december 2013 kommer Microsoft ta bort detta certifikat ur sitt rotcertifikatprogram.

Även om den gamla PKI:n kommer att fungera ytterligare en tid är det bra om arbetet med att migrera de system som använder HCC för funktion utgivna av v3 till att använda v1 certifikat istället, påbörjas så snart som möjligt. Detta för att systemen skall hinna genomgå tester där eventuella kompabilitetsproblem med v1 certifikat kan identifieras. Detta är nödvändigt då certifikat utgivna v1 har andra tekniska förutsättningar än funktionscertifikat utgivna av den gamla PKI:n, se checklistorna längre ned i detta dokument.

Det är också bra att börja förse sina medarbetare med HCC för Person utgivna från v1 Type 1, något som i vissa fall kan komma att innebära byte av SITHS-kort för medarbetaren.

Eftersom SITHS Root CA v3 vid denna brytpunkt kommer plockas bort som betrodd rotcertifikatutgivare från klienter som fått denna tillit installerad via Windows Update är det också bra att säkerställa att maskiner och personer fortfarande litar på certifikat utgivna av den gamla PKI:n. Detta kan innebära att man manuellt måste installera rotcertifikatet för v3 på både klientdatorer och på servrar om man inte är säker på det redan är så rotcertifikatet har distribuerats.

För HCC Funktion gäller:

Om er organisation har klienter med funktionscertifikat som ansluter TILL en tjänst som fortfarande använder v3 certifikat, måste det innan december 2013 säkerställas att SITHS Root CA v3 fortsatt är betrodd på dessa klientmaskiner.

Om er organisation TILLHANDAHÅLLER en tjänst måst det säkerställas att servrarna som används för driften av tjänsten fortsätter lita på v3 roten för att de skall vara nåbara av klienter (personer eller funktioner) med v3 certifikat under den gamla CA:ns hela giltighetstid.

För HCC Person gäller:

Det bör säkerställas att klienter som skall logga in på en tjänst som presenterar ett SITHS certifikat fortsätter lita på v3 roten för att undvika certifikatvarningar för slutanvändarna om tjänsten de försöker nå inte har hunnit byta till v1 certifikat.

[3] Detta skall inte blandas ihop med den SSL version som används som fortfarande är SSLv3, RFC6101, parallellt med TLS.

2. Teknik

SITHS har två olika miljöer en Produktionsmiljö och en Preprod-miljö (testmiljö).

2.1 Produktionsmiljön

Används för att skapa **skarpa** certifikat av typen SITHS Root CA v1 för person eller funktion. Denna miljö är den som är med i WebTrust's program för Certifikatutfärdare (CA). WebTrust är ett internationellt samfund som, baserat på Best Practices inom PKI, sätter ett regelverk som skall skapa tillit mellan de anslutna organisationerna.

Produktionsmiljön är också med i Microsofts program för rotcertifikatutgivare, vilket innebär att tillit till SITHS Rotcertifikat automatiskt installeras på alla Microsoft datorer om man ser till att hålla dem uppdaterade med Windows Update, något som är vitalt om man tänker sig att använda SITHS certifikat på tjänster som tillgängliggörs för exempelvis medborgare. En förutsättning för att få vara med i deras program är att man deltar i ovan nämna WebTrust.

För att få vara med i respektive program ställs höga krav på styrande dokument, säkerhet och förvaltningen av tjänsten. Alla styrande dokument finns på www.inera.se.

2.2 Preprodmiljön (testmiljön)

Används för att skapa certifikat av typen SITHS Root CA v1 PP. Dessa certifikat är avsedda att användas i **testmiljöer** och ingår inte i något av programmen nämnda under rubrik 2.1 ovan.

Det ställs inte lika stora krav på dokumentation och loggning vid skapande av dessa certifikat och tillit till dem måste alltså installeras manuellt i därtill avsedda testmiljöer.

2.3 Teknisk information

För teknisk information och sökvägar till olika resurser inom respektive miljö hänvisas till:

- Appendix B – Produktion
- Appendix C – Preproduktion
- Appendix D – Övriga CA-miljöer (SITHS CA v3)

3. Checklista – HCC som servercertifikat

De system/servrar som använder SITHS Funktionscertifikat (HCC Funktion), det vill säga för att svara på anrop från klienter, kan vara konstruerade att fungera på två olika sätt:

- Utan klientautentisering
- Med klientautentisering

Vid konfigurering av SITHS HCC på server, passa på att kontrollera att SSLv2 är avstängt på servrarna om det inte krävs av någon anledning. Detta är ett krypteringsprotokoll med lägre säkerhet.

I Appendix E finns generella instruktioner för och länkar för hur man installerar SITHS rotcertifikat i servermiljöer. För utförligare information se dokumentation från respektive leverantör då det varierar från system till system.

3.1 Utan klientautentisering

HCC Funktion på en server där klienten inte autentiseras med ett certifikat innebär att certifikatet enbart används av klienten för att

1. Verifiera att destinationen/servern är betrodd
2. Möjliggöra krypterad förbindelse (SSL/TLS, VPN över IPsec etc)

För användaren handlar det egentligen om att man inte skall får en certifikatvarning när man går till en hemsida som använder sig av ett SITHS certifikat se Appendix A. Man bör ur informationssäkerhetsperspektiv **INTE** vänja sina användare vid att klicka sig förbi denna typ av varning då det kan vara ett tecken på en förfalskad sida.

Eftersom både v1 och v3 lever kvar bör varje IT-organisation säkerställa att man **litar på båda rotcertifikaten**. Detta eftersom tjänster/system som byggs nu presenterar v1 certifikat och äldre system fortfarande kan ha kvar v3.

3.1.1 Kort checklista för servrar utan klientautentisering

3. Klientsidan måste vara förberedd på att antingen v1 eller v3 certifikat publiceras.
4. För att Systemet/Servern skall kunna slutföra en handskakning med klienten måste rotcertifikaten för både v1 och v3 vara importerade samt för v1 även de mellanliggande certifikaten för (se t.ex. RFC 5246, kapitel 7.4.2).
5. Servern/systemet måste också stödja de nya nyckelstorlekarna (2048 och 4096-bit).

Utöver ovanstående kan det vara bra att verifiera att serversidan klarar av att kunna importera ett HCC Funktion av Typ 3, dvs. med signeringsalgoritm SHA512 (SHA-2 512-bitar) detta för att säkra upp systemen för framtiden.

3.2 Med klientautentisering

I det fall man använder sig av dubbelsidig autentisering (både server och klient autentiserar sig med hjälp av certifikat) bör följande verifieras:

6. Säkerställ att systemet har kompatibilitet med de nyckellängder som används inom SITHS CA. SITHS Rotcertifikat använder sig av 4096 bitars nyckellängd. De mellanliggande CA servrarna ställer ut certifikat enligt följande:
   - Type 1 – HCC Person, 2048 bitar
   - Type 2 – HCC Funktion, 2048
   - Type 3 – HCC Funktion, 4096 bitar.

   Eftersom roten använder sig av 4096-bitars längd måste man ha kompatibilitet ända upp till 4096 bitars RSA-nycklar totalt även om man bara kommer i kontakt med HCC Person.
7. Att inloggningstjänster etablerar tillit till PKI för båda CA versionerna och kan autentisera användare från både v1 och v3, samt i förekommande fall även Crossborder CA. Det innebär alltså att båda rotcertifikaten ska vara importerade i korrekt truststore samt för v1 att också mellanliggande certifikat (typ 1, 2 och 3) ligger i därtill avsedd truststore; alternativt att mellanliggande certifikat kan laddas hem från utpekade platser i certifikatets AIA.
8. Att det går att nå de spärrtjänster som finns uppsatta för berörda CA versioner, se Appendix B, C och D.
9. Verifiera att certifikat som ni validerar vid autentisering (t.ex. inloggning med SITHS-kort, HCC Person) valideras kryptografiskt, dvs. på rätt sätt[4].
10. Utför tester över en lastad anslutning innan produktionssättning. På grund av de längre nycklarna i v1 kommer lasten på Servrar/System som utför klientautentisering att öka. En tumregel är att en dubbelt så lång nyckel tar 7 gånger längre tid att verifiera kryptografiskt. Lägg till detta att certifikatskedjan är ett steg längre än tidigare, vilket kan göra tidsaspekten avgörande för redan hårt lastade system.
11. Testa att systemet kan autentisera både anslutande parter som presenterar ett certifikat utgivet ur SITHS Root CAv1, antingen Typ 1 (HCC person) eller Typ 2 (HCC Funktion) **SAMT** certifikat utgivna av den gamla SITHS Root CA v3.

[4] Inom vården har man så sent som under hösten 2012 hittat system som bara validerar genom strängmatchning av utfärdarens namn, dvs. letar efter strängen ”SITHS v3” i certifikatet. För att få en korrekt validering bör applikationer använda ”normala” cryto-lib:ar för att göra en korrekt certifikatverifikation mot någon av SITHS revokeringsservrar.

Utöver ovanstående kan det vara bra att verifiera att serversidan klarar av att kunna importera ett HCC Funktion av Typ 3, dvs. med signeringsalgoritm SHA512 (SHA-2 512-bitar) detta för att säkra upp systemen för framtiden.

3.2.1 Testfall

Det som bör testas är att:

12. Mellanliggande certifikat levereras ut på korrekt sätt i enlighet med RFC 5246, kapitel 7.4.2.
13. Systemet klarar de längre nycklarna.
14. Systemet litar på certifikat utgivna av båda PKI:er v1 och den utgående v3.
15. Inloggningstiden fortfarande är acceptabel, både för människor (SITHS-kort med nya certifikat) samt för web services. Kraven på tillämpningarnas prestanda skiljer sig mellan v1 och v3 då v1 använder längre nycklar och även bygger en certifikatkedja.

    Ju högre frekvens man har på klientautentiseringar i sitt system desto viktigare är denna punkt.

I det fall ni har en programvara som klarar av SHA512 som signeringsalgoritm bör även certifikat av Typ 3 (HCC Funktion, SHA512) testas. Detta innebär att anrop från en klient med certifikat av typ 3 kan autentiseras.

4. Checklista – HCC klientcertifikat

Båda typer av certifikat (HCC Funktion och HCC Person) kan användas som klientcertifikat. Det kan vara maskin-till-maskin-kommunikation eller människa-till-maskin-kommunikation. Tekniskt sätt är klientcertifikatet detsamma. Det som händer i t.ex. en SSL/TLS-förbindelse är att servern efterfrågar klientcertifikatet under handskakningen.

4.1 Klient-PC

Här förutsätter vi att det är HCC person som används som klientcertifikat. De saker som kan göras och testas på klientsidan är:

4.1.1 Installera SITHS Rotcertifikat på klientdatorerna

För att inte medarbetare inte skall få varningar när de använder tjänster som har SITHS certifikat måste klientdatorerna lita på v1 samt v3. Ur informationssäkerhetssynpunkt bör man **INTE** lära användare att ”klicka sig förbi” denna typ av varningar då de kan vara ett tecken på att man kommit till en förfalskad webbsida.

Observera att de mellanliggande certifikaten för v1 inte behöver installeras när certifikatkedjan byggs med hjälp av AIA-adresserna, men att prestandan kan komma att påverkas av detta eftersom en kontroll mot AIA kommer göras.

Installationen av rotcertifikat kan göras på flera sätt varav några listas här:

16. Ladda ner rotcertifikat för v1 och v3 från Ineras hemsida (1) och installera detta på klienter via ex. Grupp principer (Group Policys) om ni har en Microsoftmiljö. Eller använd annan central distributionslösning.
17. Se till att alla klientdatorer har Windows Update **KB931125** installerad (2).
18. För att snabbt lösa problemet för enstaka användare kan ni be dem följa instruktionen för manuellt installation i Appendix A.

4.1.2 Åtkomst till spärrlistan

Se också till att det går att nå de spärrtjänster som finns uppsatta, se Appendix B, C och D. Detta för klientprogramvaran skall kunna göra revokeringskontroll mot det certifikat som Servern presenterar.

4.1.3 Testfall

Som test att ovanstående har gjorts ska klienten (läs: Internet Explorer) kunna gå till https://type3.valid.siths.se utan att få en certifikatvarning.

I det fall klientprogramvara inte är webbaserad, dvs. är egen applikation, måste tester ske i enlighet med följande:

19. Att klienten klarar nyckel längder upp till 4096-bitar både för HCC Person (klientcertifikatet) och det certifikat som serversidan presenterar.
20. Att klienten klarar av att verifiera ett HCC Funktion-certifikat av typ 2 och 3 parallellt med certifikat redan utgivna av SITHS v3.
21. Att klientprogramvaran kan verifiera spärrstatus mot revokeringstjänster angivna i Appendix B, C och D.
22. Att klientprogramvarans tid för att processa inloggning, signering, kryptering är acceptabel. Kraven på tillämpningarnas prestanda skiljer sig mellan v1 och v3 då v1 använder längre nycklar och även bygger en certifikatkedja.

4.2 Web services – klientsida

Kommunikation mellan en klient och en web service kan antingen ske:

23. Helt okrypterat
24. Genom kommunikation över en SSL/TLS-förbindelse med eller utan mutual authentication
25. Samt med eller utan Web Service Security (WSS[5]).

[5] För mer information, se t.ex. https://en.wikipedia.org/wiki/WS-Security

Beroende på var krypteringen/signering hanteras, måste tillit till de nya certifikaten hanteras i respektive trust store. Detta ligger dock utanför detta dokument, då det varierar mellan olika tillämpningar och plattformar.

5. Referenslista

1. **Inera AB.** SITHS - Root Certifikat. *Under Identifieringstjänst SITHS - Dokument - CA Certifikat.* [Online] http://www.inera.se.

2. —. SITHS - Windows Update för Godkända Root Certifikatutgivare. [Online] http://support.microsoft.com/kb/931125.

3. **Oracle.** SITHS - Trust Store - Oracle/Java. *SITHS - Trust Store - Oracle/Java.* [Online] http://docs.oracle.com/javase/1.4.2/docs/tooldocs/windows/keytool.html#importCmd.

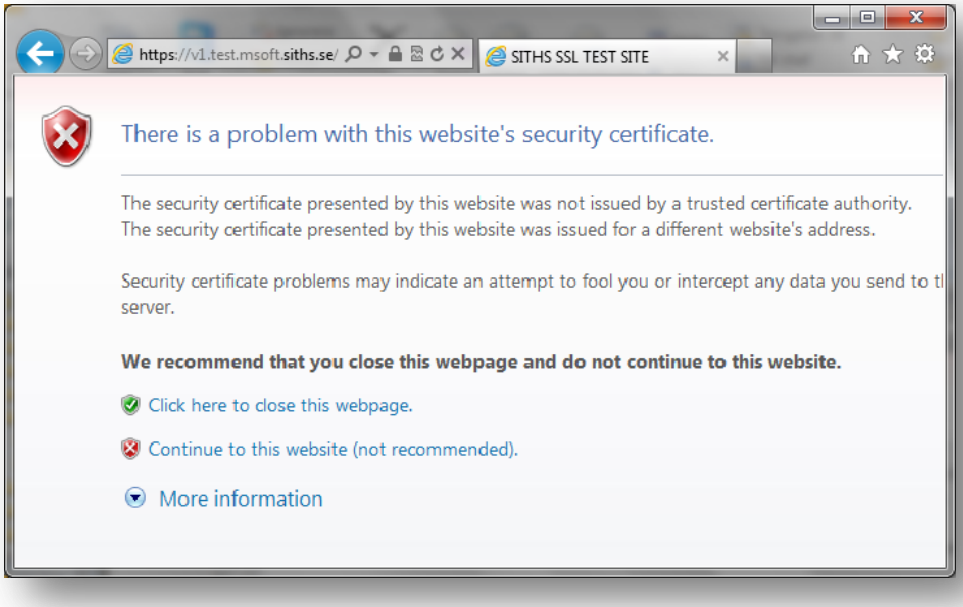
4. **JBOss.** SITHS - Truststore - JBoss. *SITHS - Truststore - JBoss.* [Online] https://docs.jboss.org/jbossweb/2.1.x/ssl-howto.html..

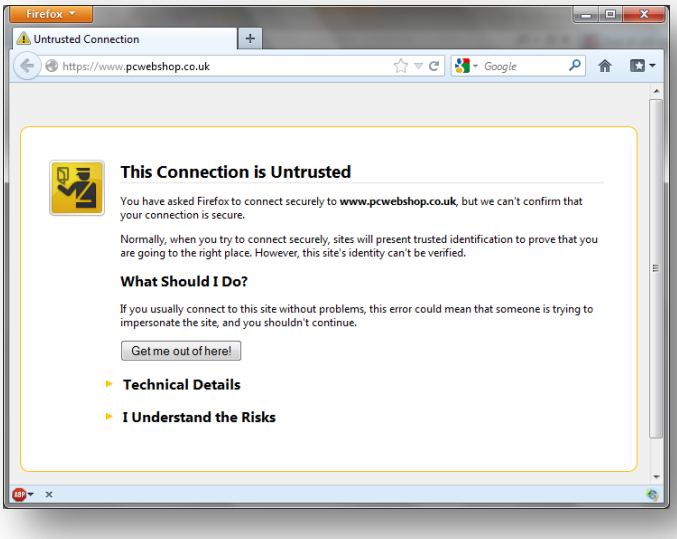
5. **IETF.** IETF SSLv3 - RFC 6101. *IETF SSLv3 - RFC 6101.* [Online] http://tools.ietf.org/html/rfc6101.

Appendix A

6. Exempel varningsmeddelande

Detta appendix fungerar som en instruktion för manuell installation av v1 på **enstaka klientdatorer.** Rotcertifikatet bör installeras på alla klientdatorer som går mot server som använder ett SITHS certifikat oavsett om det sker med eller utan klienautentisering. Om det inte är gjort möts användaren av en bild liknande de nedan:



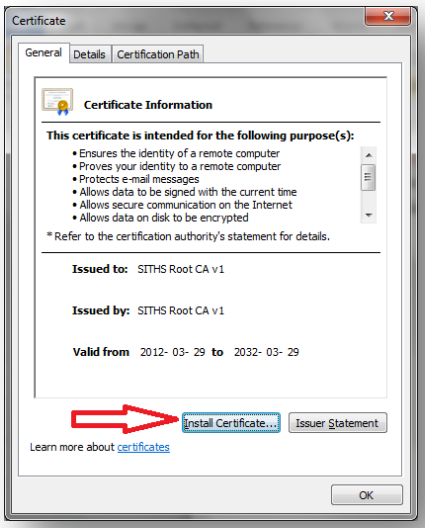


6.1 Manuell installation av SITHS Rotcertifikat på enstaka Windows-dator.

26. Identifiera vilken version av certifikat som publiceras på den tjänst som visar upp en varning.

27. Hämta hem Rotcertifikat för v1 eller v3 från Ineras hemsida (1).

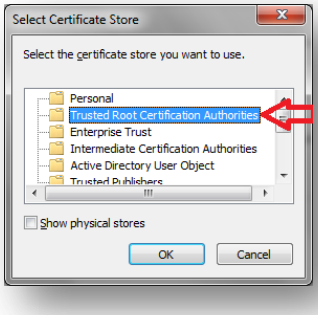
28. Dubbelklicka på filen som laddats ned



29. Klicka på fliken ”Install Certificate…”

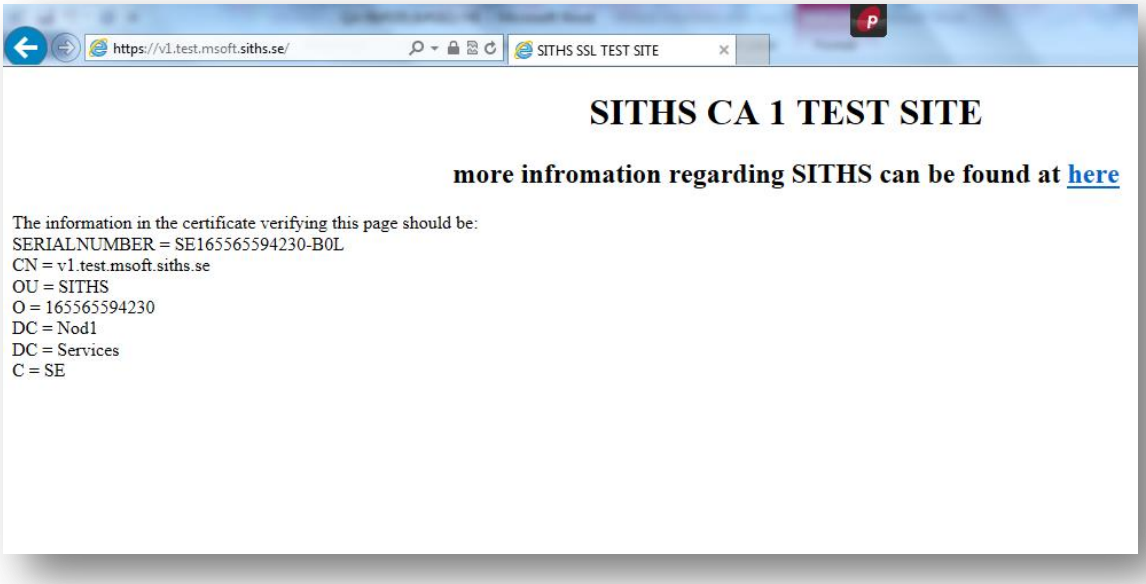
30. Tryck sedan Next, därefter kryssa i ”Place all certificates in the following store”.

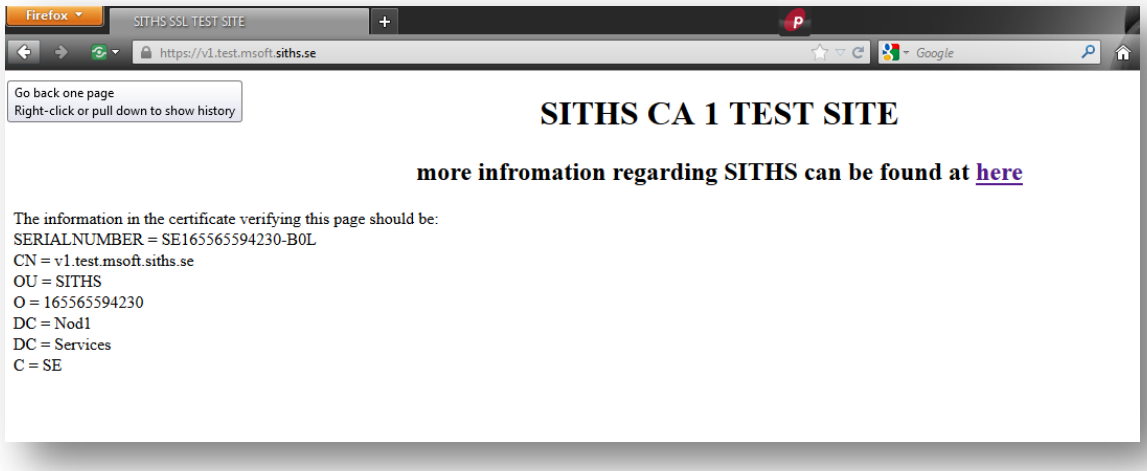
31. Klicka sedan “Browse” och Välj “Trusted Root Certification Authorities”



32. Svara OK på alla frågor som dyker upp.

33. Klart - testa att gå mot https://type3.valid.siths.se.
34. Du borde då få upp en sida utan varning som liknar de nedan:





35. Medarbetaren ska **INTE** längre mötas av en liknande bild som nedan.

Appendix B

7. SITHS Produktionsmiljö

Nedan följer ett antal länkar som är bra att känna till för SITHS produktionsmiljö och som bör vara öppna för användare baserat på i vilket syfte de använder SITHS. Administrationsgränssnittet behövs egentligen bara för medarbetare inom RA-organisationen. Sökvägarna för spärrinformation bör vara öppna både för klienter och servrar.

7.1 Brandväggsöppningar

Observera att länkar och destinationer som används för SITHS CA v3 fortfarande ska vara öppna och fungerade.

7.1.1 Sjunet

DNS-namn	IP-adress	Protokoll	Port
ccat.trust.telia.com	82.136.160.41	TCP/HTTPS	443
ccu.trust.telia.com	82.136.160.40	TCP/HTTPS	443
aia.siths.sjunet.org crl2.siths.sjunet.org	82.136.160.44	TCP/HTTP	80
ocsp2.siths.sjunet.org	82.136.160.42	TCP/HTTP	80

7.1.2 Internet

DNS-namn	IP-adress	Protokoll	Port
cve.trust.telia.com	194.237.208.172	TCP/HTTPS	443
aia.siths.se crl1.siths.se	194.237.208.239	TCP/HTTP	80
ocsp1.siths.se	194.237.208.174	TCP/HTTP	80

7.2 URL till Administrationsgränssnitten

För att nå administrationsgränssnittet för SITHS gränssnittet behöver Brandväggarna vara öppna för trafik över TCP port 443 till nedan adresser.

7.2.1 SITHS Admin

Används för att beställa Certifikat (HCC) till funktion eller person. Detta görs baserat på ett underlag som först skapas i HSA-katalogen.

- Internet - https://cve.trust.telia.com/ccat
- Sjunet – https://ccat.trust.telia.com/ccat

7.2.2 SITHS Självadmin

Används för att i efterhand eller på distans hämta ut Certifikat (HCC) till Person

- Internet – https://cve.trust.telia.com/ccu
- Sjunet https://ccat.trust.telia.com/ccu

7.3 URL Rot- och mellanliggandecertifikat

Finns att hämta på Ineras hemsida (1), alternativt direkt från de platser som anges i certifikatsinformationen:

7.3.1 Sjunet

Certifikatserver	URL
SITHS Root CA v1	http://aia.siths.sjunet.org/sithsrootcav1.cer
SITHS Type 1 CA v1	http://aia.siths.sjunet.org/sithstype1cav1.cer
SITHS Type 2 CA v1	http://aia.siths.sjunet.org/sithstype2cav1.cer
SITHS Type 3 CA v1	http://aia.siths.sjunet.org/sithstype3cav1.cer

7.3.2 Internet

Certifikatserver	URL
SITHS Root CA v1	http://aia.siths.se/sithsrootcav1.cer
SITHS Type 1 CA v1	http://aia.siths.se/sithstype1cav1.cer
SITHS Type 2 CA v1	http://aia.siths.se/sithstype2cav1.cer
SITHS Type 3 CA v1	http://aia.siths.se/sithstype3cav1.cer

7.4 URL för Revokeringskontroll

All kontroll av revokering sker via TCP port 80, HTTP.

7.4.1 Sjunet

Revokeringstjänst	URL
OCSP för alla certifikat	http://ocsp2.siths.sjunet.org
CRL – Personcertifikat (Type 1)	http://crl2.siths.sjunet.org/sithstype1cav1.crl
CRL – Funktionscertifikat (Type 2)	http://crl2.siths.sjunet.org/sithstype2cav1.crl
CRL – Funktionscertifikat (Type 3)	http://crl2.siths.sjunet.org/sithstype3cav1.crl
CRL – Mellanliggande certifikatservrar	http://crl2.siths.sjunet.org/sithsrootcav1.crl

7.4.2 Internet

Revokeringstjänst	URL
OCSP för alla certifikat	http://ocsp1.siths.se
CRL – Personcertifikat (Type 1)	http://crl1.siths.se/sithstype1cav1.crl
CRL – Funktionscertifikat (Type 2)	http://crl1.siths.se/sithstype2cav1.crl
CRL – Funktionscertifikat (Type 3)	http://crl1.siths.se/sithstype3cav1.crl
CRL – Mellanliggande certifikatservrar	http://crl1.siths.se/sithsrootcav1.crl

Appendix C

8. SITHS Preprod-miljö

SITHS har också en så kallad Preprod-miljö i vilken man kan ta ut certifikat för **test**. Dessa **PP-certifikat** är i princip identiska med de certifikat som utfärdas i produktionsmiljön och är utgivna från en likadan PKI-struktur.

Preprod-miljön ingår inte i Microsofts Root CA program och kräver därför inte samma handläggning avseende rutiner och hantering av Certifikat och Kort. Dock ligger ansvaret fortfarande på respektive RA-organisation att hålla ordning i sin gren. Dessutom blir det lättare att flytta över det man gjort i Test till Produktion om man försöker hålla miljöerna så lika varandra som möjligt.

De skillnader som finns mellan miljöerna är namnsättningen där man i Preprod lägger på suffixet **PP**, det vill säga rot-certifikatet kallas för **SITHS Root CA v1 PP** och utfärdar-certifikatet för Typ 1-certifikat (HCC Person) kallas för **SITHS Type 1 CA v1 PP**.

Alla variabler, nyckellängder mm är precis likadana, med den skillnaden att revokeringskontroll genom OSCP, CDP och AIA[6] görs av PP-servrar istället. Detta gör att man måste göra ytterligare brandväggsöppningar för revokeringskontroll för system som använder Preprod certifikat.

8.1 Brandväggsöppningar

8.1.1 Sjunet

DNS-namn	IP-adress	Protokoll	Port
ccat.preprod.trust.telia.com	82.136.160.51	TCP/HTTPS	443
ccu.preprod.trust.telia.com	82.136.160.50	TCP/HTTPS	443
aiapp.siths.sjunet.org crl2pp.siths.sjunet.org	82.136.160.53	TCP/HTTP	80
ocsp2pp.siths.sjunet.org	82.136.160.52	TCP/HTTP	80

[6] OCSP = Online Certificate Status Protocol

CDP = CRL distribution point

AIA = Authority Information Access

8.1.2 Internet

DNS-namn	IP-adress	Protokoll	Port
cve.preprod.trust.telia.com	194.237.208.168	TCP/HTTPS	443
aiapp.siths.se crl1pp.siths.se	194.237.208.238	TCP/HTTP	80
ocsp1pp.siths.se	194.237.208.170	TCP/HTTP	80

8.2 URL till Administrationsgränssnitten

För att nå administrationsgränssnittet för SITHS gränssnittet behöver Brandväggarna vara öppna för trafik över TCP port 443 till nedan adresser.

8.2.1 SITHS Admin

Används för att beställa Certifikat (HCC) till funktion eller person. Detta görs baserat på ett underlag som först skapas i HSA-katalogen.

- Internet - https://cve.preprod.trust.telia.com/ccat
- Sjunet – https://ccat.preprod.trust.telia.com/ccat

8.2.2 SITHS Självadmin

Används för att i efterhand eller på distans hämta ut Certifikat (HCC) till Person

- Internet – https://cve.preprod.trust.telia.com/ccu
- Sjunet https://ccu.preprod.trust.telia.com/ccu

8.3 URL Rot- och mellanliggandecertifikat

Finns att hämta på Ineras hemsida (1), alternativt direkt från de platser som anges i certifikatsinformationen:

8.3.1 Sjunet

Certifikatserver	URL
SITHS Root CA v1 PP	http://aiapp.siths.sjunet.org/sithsrootcav1pp.cer
SITHS Type 1 CA v1 PP	http://aiapp.siths.sjunet.org/sithstype1cav1pp.cer
SITHS Type 2 CA v1 PP	http://aiapp.siths.sjunet.org/sithstype2cav1pp.cer
SITHS Type 3 CA v1 PP	http://aiapp.siths.sjunet.org/sithstype3cav1pp.cer

8.3.2 Internet

Certifikatserver	URL
SITHS Root CA v1 PP	http://aiapp.siths.se/sithsrootcav1pp.cer
SITHS Type 1 CA v1 PP	http://aiapp.siths.se/sithstype1cav1pp.cer
SITHS Type 2 CA v1 PP	http://aiapp.siths.se/sithstype2cav1pp.cer
SITHS Type 3 CA v1 PP	http://aiapp.siths.se/sithstype3cav1pp.cer

8.4 URL för Revokeringskontroll

All kontroll av revokering sker via TCP port 80, HTTP.

8.4.1 Sjunet

Revokeringstjänst	URL
OCSP för alla certifikat	http://ocsp2pp.siths.sjunet.org
CRL – Personcertifikat (Type 1)	http://crl2pp.siths.sjunet.org/sithstype1cav1pp.crl
CRL – Funktionscertifikat (Type 2)	http://crl2pp.siths.sjunet.org/sithstype2cav1pp.crl
CRL – Funktionscertifikat (Type 3)	http://crl2pp.siths.sjunet.org/sithstype3cav1pp.crl
CRL – Mellanliggande certifikatservrar	http://crl2pp.siths.sjunet.org/sithsrootcav1pp.crl

8.4.2 Internet

Revokeringstjänst	URL
OCSP för alla certifikat	http://ocsp1pp.siths.se
CRL – Personcertifikat (Type 1)	http://crl1pp.siths.se/sithstype1cav1pp.crl
CRL – Funktionscertifikat (Type 2)	http://crl1pp.siths.se/sithstype2cav1pp.crl
CRL – Funktionscertifikat (Type 3)	http://crl1pp.siths.se/sithstype3cav1pp.crl
CRL – Mellanliggande certifikatservrar	http://crl1pp.siths.se/sithsrootcav1pp.crl

Appendix D

9. Övriga CA-miljöer

Det finns ett antal äldre CA miljöer varan en del fortfarande är i bruk och kommer att användas en tid framöver:

- **SITHS CA CrossBorder** – Används för att skapa funktionscertifikat för Personer som inte har svenskt personnummer.
- **SITHS CA CrossBorder TEST v3** - Används för att skapa funktionscertifikat för Personer som inte har svenskt personnummer.

Medan en del är under avveckling och beskrivs mest för att det fortfarande finns en stor mängd person- och funktionscertifikat utgivna från dem:

- SITHS CA TEST v4

9.1 Brandväggsöppningar

9.1.1 Sjunet (Produktion)

DNS-namn	IP-adress	Protokoll	Port
ccat.trust.telia.com	82.136.160.41	TCP/HTTPS	443
ccu.trust.telia.com	82.136.160.40	TCP/HTTPS	443
sithscrl.carelink.sjunet.org	82.136.160.54	TCP/LDAP	389
sithsocsp.trust.telia.com (CNAME) till **ocspv3.siths.sjunet.org**	**82.136.160.42** om frågan ställs VIA Sjunet	TCP/HTTP	80

9.1.2 Internet (Produktion)

DNS-namn	IP-adress	Protokoll	Port
cve.trust.telia.com	194.237.208.172	TCP/HTTPS	443
www.carelink.se	194.237.208.239	TCP/HTTP	80
sithsocsp.trust.telia.com (CNAME) till **ocspv3.siths.sjunet.org**	**194.237.208.174** om frågan ställs VIA Internet	TCP/HTTP	80

9.1.3 Sjunet (Preprod)

URL (IP-adress)	IP-adress	Protokoll	Port
ccat.preprod.trust.telia.com	82.136.160.51	TCP/HTTPS	443
ccu.preprod.trust.telia.com	82.136.160.50	TCP/HTTPS	443
sithscrl.carelink.sjunet.org	82.136.160.54	TCP/LDAP	389
sithsocsp.preprod.trust.telia.com (CNAME) till **ocspv3.preprod.siths.sjunet.org**	**82.136.160.52** om frågan ställs VIA Sjunet	TCP/HTTP	80

9.1.4 Internet (Preprod)

URL (IP-adress)	IP-adress	Protokoll	Port
cve.preprod.trust.telia.com	194.237.208.168	TCP/HTTPS	443
www.carelink.se	194.237.208.239	TCP/HTTP	80
sithsocsp.preprod.trust.telia.com (CNAME) till **ocspv3.preprod.siths.sjunet.org**	**194.237.208.170** om frågan ställs VIA Internet	TCP/HTTP	80

9.2 URL till Administrationsgränssnitten

För att nå administrationsgränssnittet för SITHS gränssnittet behöver Brandväggarna vara öppna för trafik över TCP port 443 till nedan adresser.

9.2.1 SITHS Admin

Används för att beställa Certifikat (HCC) till funktion eller person. Detta görs baserat på ett underlag som först skapas i HSA-katalogen.

- Internet - https://cve.trust.telia.com/ccat
- Sjunet – https://ccat.trust.telia.com/ccat

9.2.2 SITHS Självadmin

Används för att i efterhand eller på distans hämta ut Certifikat (HCC) till Person

- Internet – https://cve.trust.telia.com/ccu
- Sjunet https://ccat.trust.telia.com/ccu

9.3 URL Rotcertifikat

Finns att hämta på Ineras hemsida (1)

9.4 URL för Revokeringskontroll

Internet - All kontroll av revokering sker via TCP port 80, HTTP

Sjunet – Kontroll av revokering sker antingen via:

- TCP port 389, LDAP
- TCP port 80, HTTP (OCSP)

9.4.1 Sjunet

Revokeringstjänst	URL
OCSP för alla certifikat	(CNAME) http://sithsocsp.trust.telia.com --> http://ocspv3.siths.sjunet.org, se Förklaring av OCSP för äldre CA's.
CRL – SITHS CA v3	ldap://sithscrl.carelink.sjunet.org/cn=SITHS%20CA%20ver%203,o=SITHS%20CA,c=SE?certificateRevocationList;binary?
CRL – Crossborder	ldap://sithscrl.carelink.sjunet.org/cn=SITHS CA CrossBorder ,o=SITHS CA,c=SE?certificateRevocationList;binary
CRL – Crossborder TEST v3	ldap://sithscrl.carelink.sjunet.org/cn=SITHS CA CrossBorder TEST v3, o=SITHS CA, c=se?certificateRevocationList;binary
CRL – SITHS CA v3 TEST	ldap://sithscrl.carelink.sjunet.org/cn=SITHS CA TEST v3,o=SITHS CA,c=se?certificateRevocationList;binary
CRL – SITHS CA v4 TEST	ldap://sithscrl.carelink.sjunet.org/cn=SITHS CA TEST v4,o=SITHS CA,c=se?certificateRevocationList;binary

9.4.2 Internet

Revokeringstjänst	URL
OCSP för alla certifikat	(CNAME) http://sithsocsp.trust.telia.com --> http://ocspv3.siths.sjunet.org, se Förklaring av OCSP för äldre CA's.
CRL – SITHS CA v3	http://www.carelink.se/siths-ca/ca003.crl
CRL – Crossborder	http://www.carelink.se/siths-ca/ca004.crl
CRL – Crossborder TEST v3	http://www.carelink.se/siths-ca/test-crl004.crl
CRL – SITHS CA v3 TEST	http://www.carelink.se/siths-ca/test-

	crl0003.crl
CRL – SITHS CA v4 TEST	http://www.carelink.se/siths-ca/test-crl0006.crl

9.5 Förklaring av OCSP för äldre CA's

Eftersom det bara finns ett DNS-värde för OCSP servern utpekat i certifikaten har denna historiskt pekats till servern på Internet varav OCSP frågor över Sjunet inte har varit möjlig för denna CA utan egen konfigurering i den interna miljön.

Sedan december 2012 har dock en förändring gjorts som gör att beroende på över vilket nät DNS-frågan ställs så får man olika svar beroende på om det är via Sjunet eller Internet.

sithsocsp.trust.telia.com som pekas ut i certifikaten är i själva verket ett CNAME till **ocspv3.siths.sjunet.org** som ger följande IP-adresser beroende på över vilket nät frågan ställs till Sjunets DNS-servrar:

- Internet – ocspv3.siths.sjunet.org (194.237.208.170)
- Sjunet – ocspv3.siths.sjunet.org (82.136.160.42)

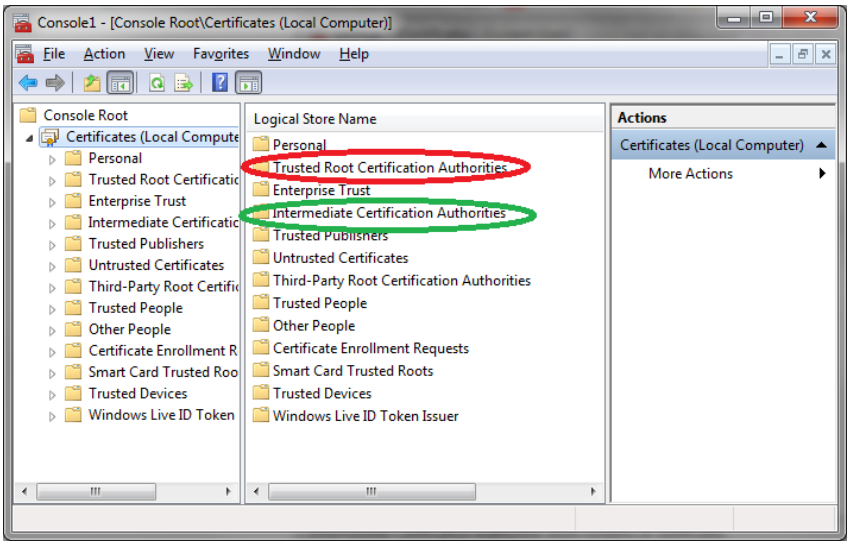
Appendix E

10. Exempel - Installera rotcertifikat i truststore

Alla applikationer använder sig av olika trust stores, allt är beroende på hur man har implementerat i koden. Nedan visas hur man lägger till rot-certifikatet i Windows truststore.

10.1 Windows

Windows använder sig av olika truststore, beroende på vilket konto som ska nå certifikaten. För System/Servrar används antingen den store som är knuten till Local Computer eller den som är knuten till respektive tjänst. Detta är beror på hur man har byggt upp sin tjänst.



För att lita på nya rotcertifikat installeras dessa i den container som är rödmarkerad på bilden ovan. De mellanliggande certifikaten som används inom PKI:n för v1 läggs in i den container som är grönmarkerad.

Därefter ser man till att servern kan nå de spärr- och valideringsservrar som är uppsatta, se Appendix B, C och D.

10.2 Java

En javamiljö har både en keystore (nyckellagring) och en truststore (rotcertifikatslagring). I det fall man vill att en java-tillämning ska lita på certifikat som är utgivna av en ny PKI (i detta fall den nya SITHS), så måste motsvarande rot-certifikat importeras i truststore. Den standard-mässiga platsen för truststore är filen cacerts som ligger i java.home\lib\security\.

Verktyget att importera fler certifikat till denna lagringsfil är keytool. Observera att varje javaapplikation kan peka ut annan truststore (och keystore) än den som är standard.

Observera också att certifikatskedjan (rot- och mellanliggande certifikat) måste installeras.

Se mera på Oracle's hemsida (3)

Därefter ser man till att systemet kan nå de spärr- och valideringsservrar som är uppsatta, se Appendix B, C och D.

10.3 JBoss

En tillämpning av Java är JBossWebb för dokumentation till denna plattform se JBoss hemsida (4)

Utöver detta, ser man att servern kan nå de spärr- och valideringsservrar som är uppsatta, se Appendix B, C och D.