Kerberos baserad Single Sign On, tillämpningsexempel

För att logga in i en webbapplikation med hjälp av en AD baserad autentisering behöver alla komponenter anpassas för detta.

Denna instruktion skall ses som ett extra stöd för införandet av kortbaserad SITHS inloggning, men kan naturligtvis även användas för andra typer av domänautentisering.

Förutsättningar

Denna instruktion utgår ifrån att en klient med en fungerande NetID installation och ett aktivt SITHS-kort finns att tillgå. Instruktionen förutsätter också att läsaren är väl förtrogen med AD och administrationen av denna.

En gemensam tid förutsätts i hela SSO-domänen.

Den webserver som skall användas är konfigurerad med SSL och ett SITHS certifikat.

Vad skall ske

- AD konfigureras med en GPO för att automatiskt konfigurera Internet Explorer.
- Firefox och andra web browsers konfigureras för att hantera kerberos
- IIS webserver på Win2008 konfigureras för Kerberos autentisering
- Testa att logga in i domänen och sedan kunna logga in mot web-servern
- Apache på en Linux-plattform konfigureras för Kerberos autentisering

Klientkonfigurationer

Internet Explorer

En förutsättning för att en Internet Explorer över huvud taget skall försöka använda en kerberos ticket för autenticering mot en server är att den servern betraktas som intern.

Att den är intern visas genom att kortformen av namnet används, eller att webservern är definierad att tillhöra zonen ”Lokalt Intranet”/”Intranet Zone”.

Detta kan hanteras på två sätt. Endera instrueras användaren att själv konfigurera detta i sin PC, eller så används en GPO för att administrera detta centralt.

GPO för Intranet Zone

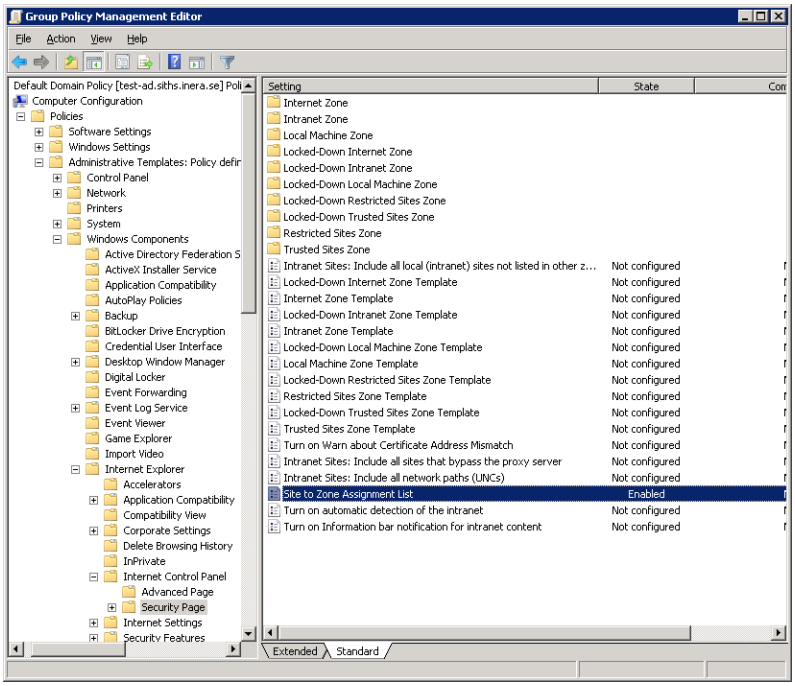
När en större mängd klienter skall konfigureras och i en centralt hanterad windowsmiljö görs dessa inställningar enklast via en GPO i AD:t.

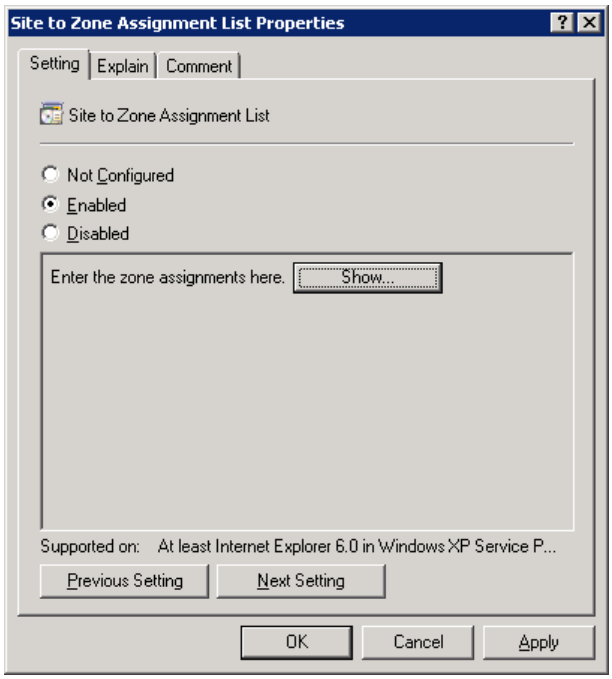
Observera: Om denna policy sätts kommer användarna själva inte längre själva kunna modifiera domäner och sites i sina maskiner. All hantering av IE-zonerna kommer att styras centralt.

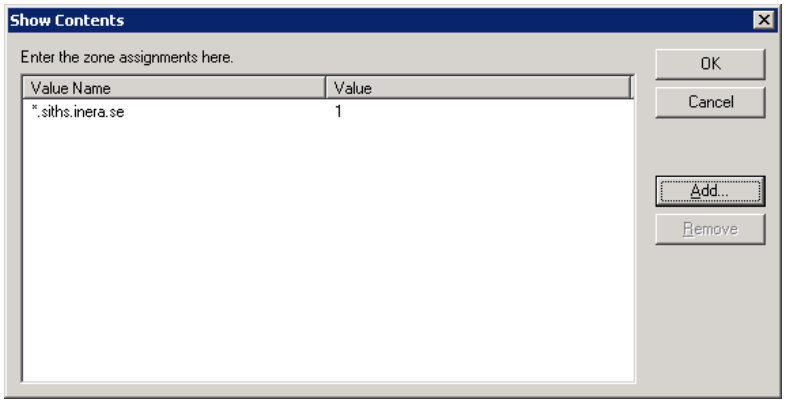
Gå till: Computer Configuration -> Aministrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page.

Editera "Site to Zone Assignment List" och lägg till intranätsdomänen.

Varje zon representeras av ett numeriskt värde, där 1 används för "Intranet Zone"

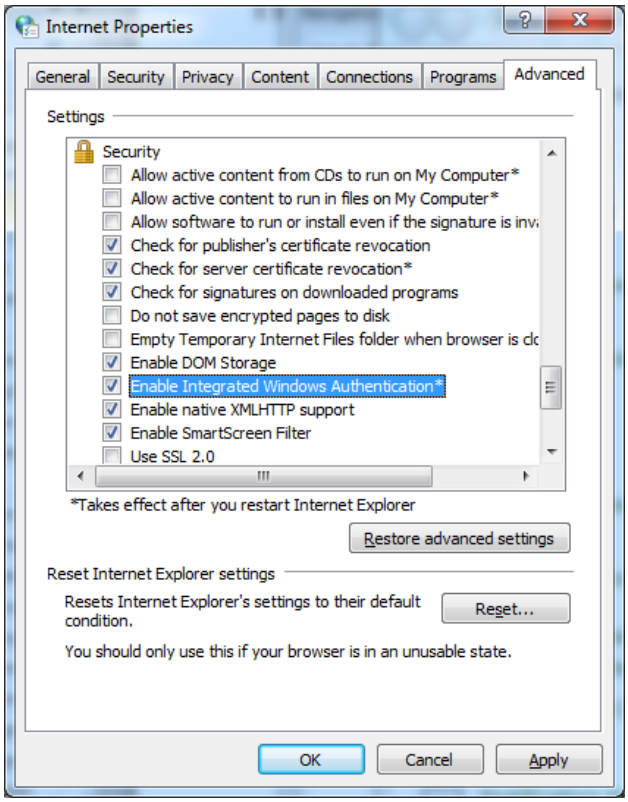




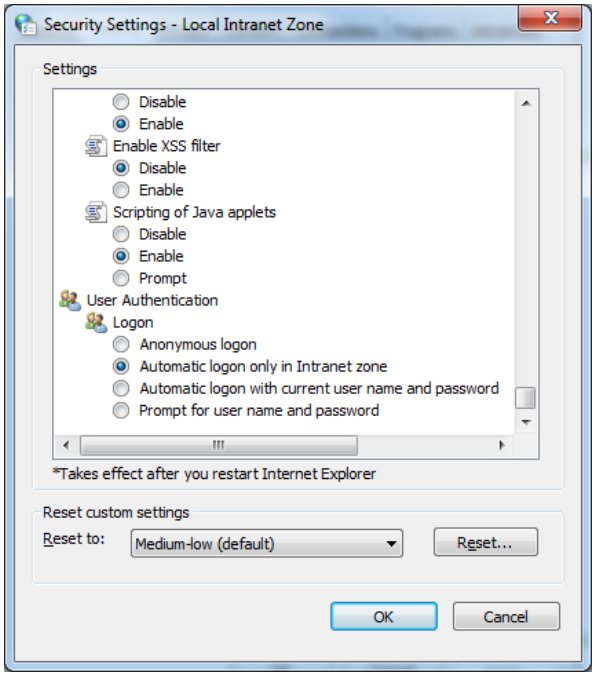


Integererad Windowsautenticering

Verifiera att ”Integrated Windows Authentication” är aktiverad på klienterna, (vilket den bör vara default)



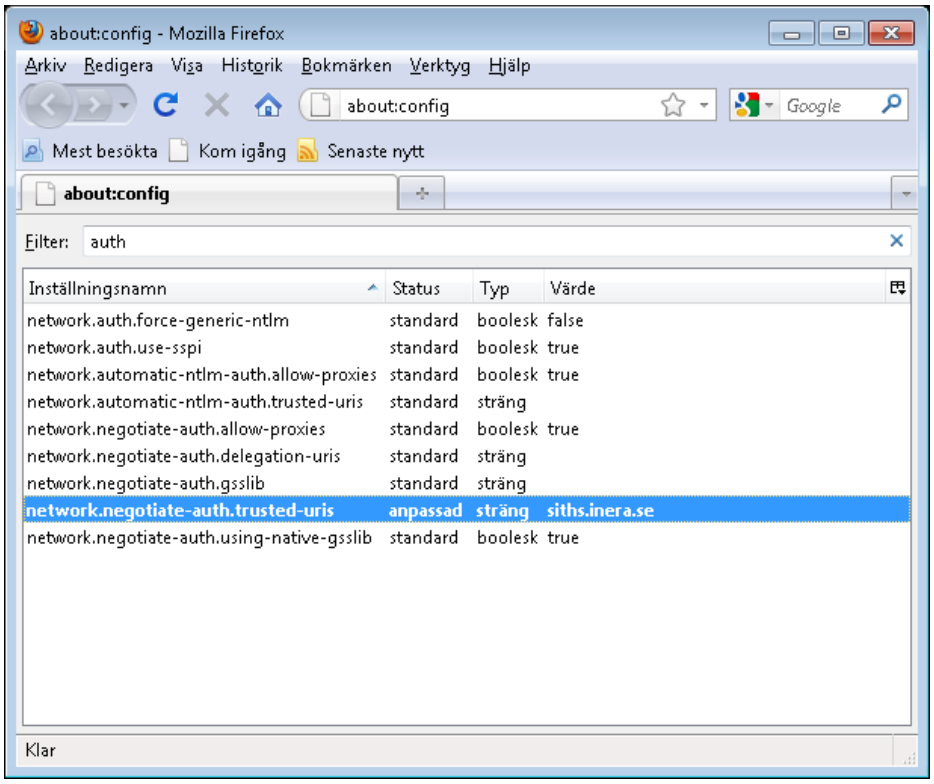
Verifiera att ”Automatic logon only in Intranet zone” är valt (vilket den bör vara default).



Firefox

För Firefox måste en konfiguration göras i varje browser, om man inte har verktyg för att provisionera firefoxinstallationspaketet i förväg.

Konfigureringen görs i about:config i strängen ***network.negotiate-auth.trusted-uris***



Referenser

1. Guidelines for enabling smart card logon with third-party certification authorities http://support.microsoft.com/kb/281245
2. How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store http://support.microsoft.com/kb/295663/
3. Requirements for Domain Controller Certificates from a Third-Party CA http://support.microsoft.com/kb/291010/

inera

SSO – Singel Sign On

Vad är SSO? Ja, det har ju med inloggning att göra och det ska helst ske bara en (single) gång, då är det bra. Men vad menar man med "SSO" inom SITHS? Menar vi samma sak som CA, Citrix, Cybercom, Oracle, Microsoft, IBM, NordicEdge? Nej, SITHS menar inte riktigt samma sak!

”SSO är den varma känsla som kan infinna sig hos en användare som på ett enkelt sätt når merparten av den information som behövs för arbetets utförande”

Om enkel inloggning ska byggas, så lär det behövas tid, kompetens, kod, system, applikationer, biljetter, pengar och handfast projektledning. Man vill självklart dra nytta av de smarta kort man införskaffat, både avseende säkerhet men framförallt gällande enkelheten för användarna.

Wikipedia på svenska

Single sign-on, SSO, är en metod inom sammansatta datasystem för att hantera användare med aspekt på användarbehörighet (auktorisering) och användarverifiering (autentisering), så att dessa användare endast behöver logga in en enda gång för att nå de system som är anpassade till tjänsten. Fördelen för användaren är att man inte behöver hålla reda på flera olika lösenord.

Wikipedia på engelska (ganska lika men med ett viktigt tillägg)

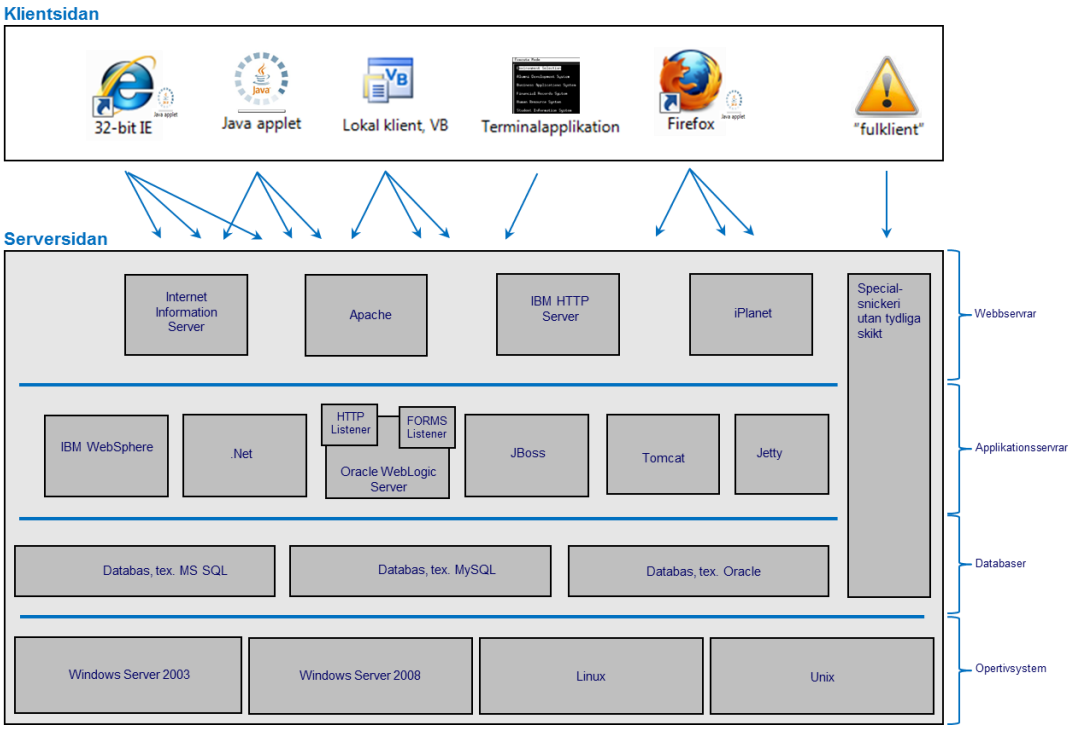
Single sign-on (SSO) is a property of access control of multiple, related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. Single sign-off is the reverse property whereby a single action of signing out terminates access to multiple software systems.

As different applications and resources support different authentication mechanisms, single sign-on has to internally translate to and store different credentials compared to what is used for initial authentication.

Alla applikationer som baserar sin autentisering på AD/Kerberos har möjlighet att utnyttja Single Sign On funktionen som en MS AD domän tillgängliggör.

För alla Microsoft-baserade och AD enablade applikationer är detta redan uppfyllt, men även andra leverantörers program och applikationer kan utnyttja detta. Hur denna funktion konfigureras är applikationsberoende och därför något som måste undersökas per applikation.

Figur 1 visar några exempel på olika applikationskoncept som kan förekomma i en tänkt infra-struktur. Floran av lösningar är stor både på klientsidan och på serversidan. Det är i denna struktur som man ska försöka åstadkomma SSO baserat på ”två-faktorsautentisering”.



Figur 1. Applikationer med behov av strukturerad inloggningsmekanism.

I en stor organisation med många olika typer av arbetsuppgifter och personalkategorier hittar man nästan undantagslöst ett stort antal applikationer som implementerat olika typer av inloggningsmekanismer, men vanligast är att användaren matar in användarnamn och lösenord.

När man har klart för sig vilka applikationer som berörs och olika inloggningssätt de använder bör man staka ut en strategi för att den kommande SSO-lösningen inte ska behöva bli spretigare än nödvändigt. Denna strategi är helt nödvändig för att kunna fatta beslut om vägen framåt. Till att börja med behöver det inte vara mer omfattande än att man ställer upp en enkel matris, som dock bör grunda sig på följande frågor:

- Hur många dispenser från SSO-känslan "tål" användarna?
- Hur pigga är våra applikationsleverantörer på att BIF-, SAML, Kerberos- smartkort-ifiera sina applikationer?
- Kan vi hitta referenser rörande lyckade SSO-projekt som vi kan ge oss värdefull input?

En prioritetsordning skulle kunna vara enligt principen:

- I första hand
  Den primära autenticeringen sker med kort/certifikat, då kan många applikationer dra nytta av denna primära inloggning (ofta mot AD) genom att applikationerna använder Kerberos.

- I andra hand
  I vissa fall sker ingen påloggning mot AD med kortet och ingen Kerberosbiljett finns tillgänglig. Då kan en SAML-baserad lösning med en intern ”Identity Provider” passa. För externa kopplingar mellan huvudmän används BIF som är ett SAML-baserat koncept.
- I tredje hand
  Certifikats-enabla applikationen
- I fjärde hand
  Nyttja en SSO-programvara som hanterar automatisk ifyllnad av namn och lösenord
- I femte hand
  Ge applikationen dispens och förklara samtidigt varför just denna applikation visat sig "hopplös".

Figur 2 visar ett exempel på hur man kan resonera kring vägen framåt för olika applikationer relaterat en tänkt infrastruktur.

	Nuvarande inloggnings-metod	Stöd finns direkt i produkten för dessa metoder	Noteringar	Beslut
Active Directory	Namn och lösen	1. Namn och lösen 2. Smarta kort med certifikat 3. Biometri 4. Osv.	Utred och fatta beslut om vi ska använda HCC eller egenutfärdade mot AD	§1 Alla med ”egen” dator ska logga på AD med smarta kort och certifikat §2 På delade datorer ska koncept för ”hot desktop” och/eller terminalsessioner användas. Påbörja införande av tunna klienter i lämpliga delar av verksamheten
Journalsystem 5.2	Namn och lösen	1. Namn och lösen 2. AD Kerberos aware 3. Direkt nyttjande av SITHS/HCC	I väntan på att alla får sina kerberosbiljetter baserat på kortinloggning överväger vi att logga på med kort direkt.	§1 Ta reda på mer om hur leverantörens lösning för kortinloggning fungerar. Hur hanteras t.ex. SITHS-kort med multipla HCC?
Personalhantering 3.0	Namn och lösen	1. Namn och lösen 2. AD Kerberos aware	-	§1 Nyttja kerberosfunktionaliteten oavsett om påloggning skett med namn/lösen eller kort
Tidredovisning 3.0	Namn och lösen	1. Namn och lösen 2. SAML	Vi är inte redo för SAML då vi saknar lämplig federationsmotor	§1 Ta reda på om vi har licens för Citrix Password Manager. Titta även på CA och IBM:s koncept för SSO.
Schemaläggning 7.1	Namn och lösen	1. Namn och lösen 2. OTP-SMS	Schemaläggning 7.1 skall fasas ut under 2011 till förmån för SchemeMaster 2.0	§1 Kontrollera vilka inloggningsmetoder SchemeMaster stödjer
NPÖ 1.1	Dubbelriktad SSL med SITHS/HCC	1. Dubbelriktad SSL med SITHS/HCC 2. BIF	BIF i skrivande stund inte helt klart	§1 Fortsätt med dubbelriktad SSL med SITHS/HCC
Specialsystem X	NTLM	1. NTLM	-	§1 Kontakta leverantören och sondera möjligheterna till en modernisering i kommande releaser
e-Dos	Namn och lösen	1. Dubbelriktad SSL med SITHS/HCC 2. Säkerhetsdosa (OTP) 3. Dubbelriktad SSL med e-legitimation	-	§1 Övergång till dubbelriktad SSL med SITHS/HCC sker när SITHS-korten är utrullade till berörd personal och så snart Apoteket infört påloggning med HCC istället för dagens påloggning med e-legitimation.

Figur 2. Beslutsmatris för SSO.

Kontentan är att om man inte går igenom sin applikationsflora och skapar en strategi för den så får man inte den nytta av sin nya PKI-infrastruktur baserad på smarta kort med certifikat som man hade hoppats. SSO är inget som kommer med PKI-tekniken i sig själv.

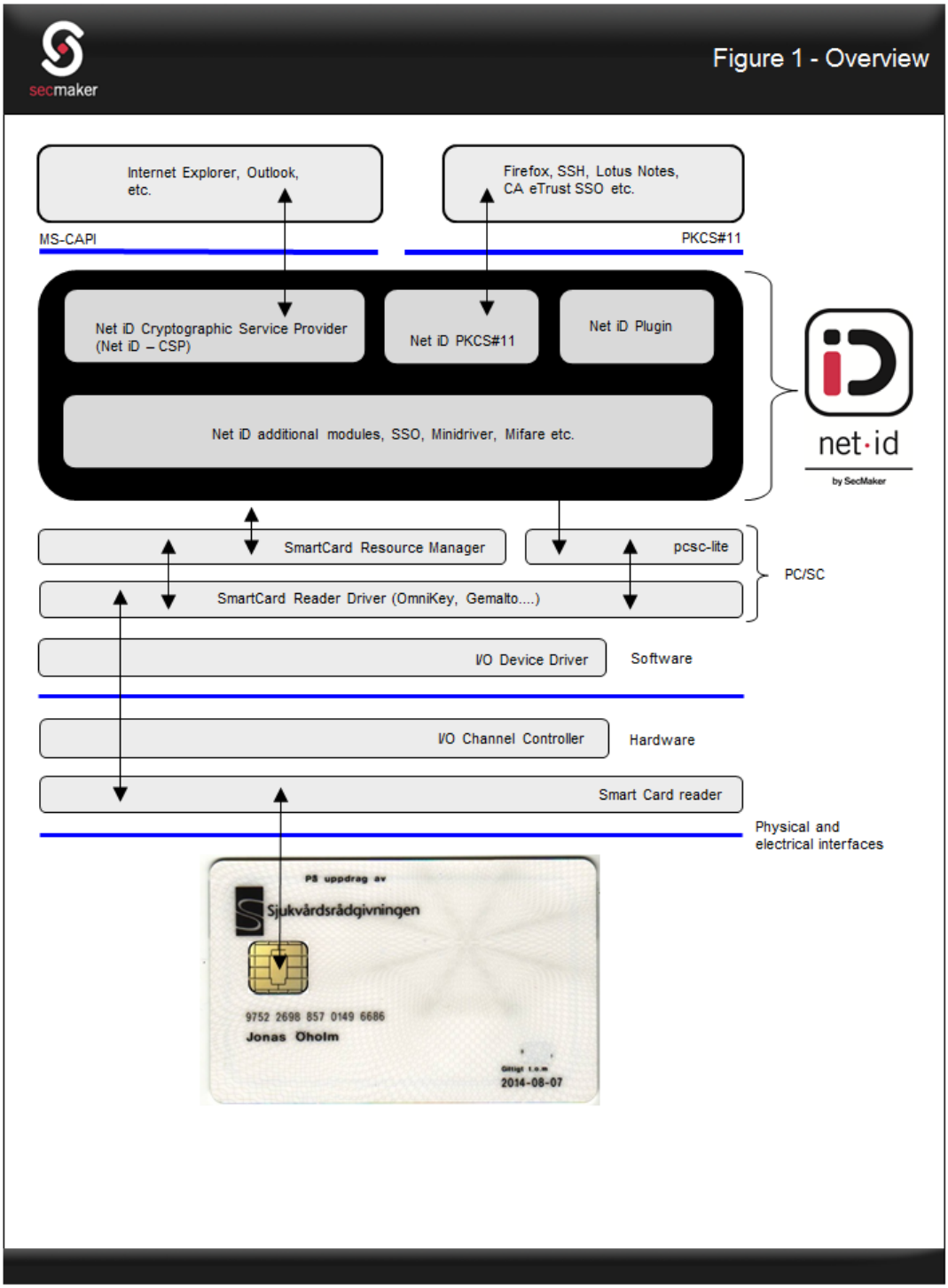
I vissa fall kan certifikatsanpassningen av en applikation bedömas vara den bästa lösningen. Rätt gjort kommer då SSO-känslan automatiskt om man tillser att man inte behöver ange PIN-koden för inloggning annat än om så explicit krävs.

Tyvärr räcker det i SITHS-sammanhang inte med att applikationen är kapabel att nyttja certifikat, den måste kunna nyttja ett certifikat som finns på ett smart kort. Exempel på applikationer som förvisso kan nyttja ett certifikat, men inte om de ligger på ett smart kort och via Net iD görs tillgängliga via MS-CAPI och/eller PKCS#11 är webbläsaren Opera och samarbetsverktyget FirstClass som båda endast kan arbeta med filbaserade nyckel/certifikatslager i sina nuvarande versioner. En överblick illustreras i figur 3.

Det finns två huvudvägar för en integration:

- Via MS-CAPI, se figur 4
- Via PKCS#11, se figur 5

Väljer man MS-CAPI så blir lösningen endast tillgänglig för Windows-plattformen. Väljer man PKCS#11 så blir lösningen tämligen plattformsoberoende. Oavsett vilken väg man väljer rekommenderar SITHS att man lägger viss möda på certifikavalslogiken för att ta höjd för en situation där mer än ett certifikat svarar mot de krav man ställt upp för inloggningen i tekniskt hänseende. Vidare kan man påpeka att det är smidigare att jobba med certifikat än att ge sig i kast med en integration på nyckelnivå via Key Containers och tokens. Slutligen bör nämnas att lösningen bör göras konfigurerbar avseende vilka utfärdare som ska accepteras samt vilket/vilka fält som ska utgöra användarbegreppet. Troligen innehåller inte certifikaten ett användarbegrepp som direkt kan användas i applikationen.



Figur 3. Översikt: SITHS kortets kommunikation med IT system och applikation.

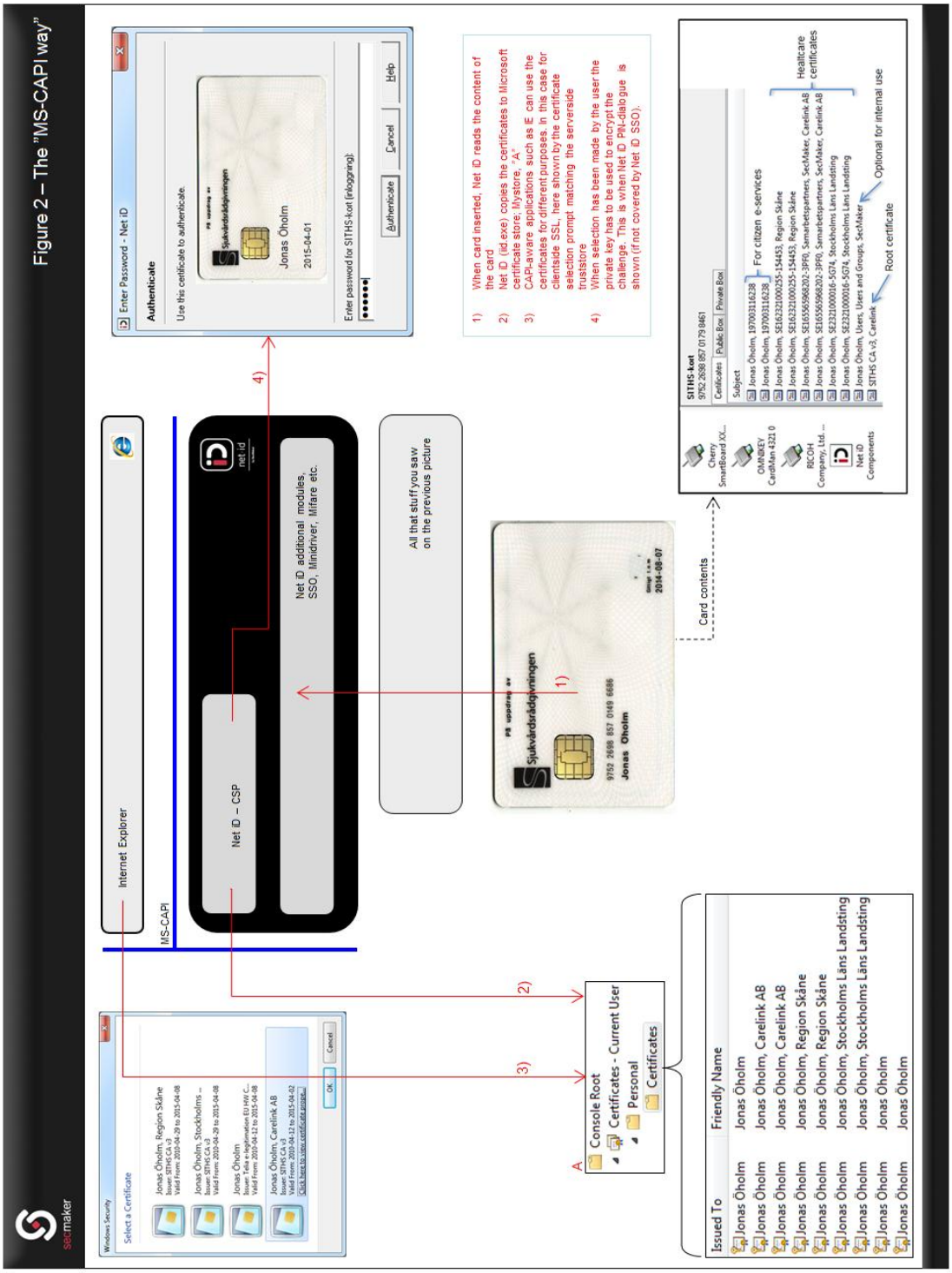


Figure 2 – The "MS-CAPI way"
Internet Explorer
MS-CAPI
Net iD – CSP
Net iD additional modules, SSO, Minidriver, Mifare etc.
All that stuff you saw on the previous picture
Enter Password - Net iD
Authenticate
Use this certificate to authenticate.
Jonas Öholm
2015-04-01
Enter password for SITHS-kort (inloggning):
Authenticate
Cancel
Help
1) When card inserted, Net iD reads the content of the card
2) Net iD (iid.exe) copies the certificates to Microsoft certificate store; Mystore, "A"
3) CAPI-aware applications such as IE can use the certificates for different purposes. In this case for clientside SSL, here shown by the certificate selection prompt matching the serverside trustistore
4) When selection has been made by the user the private key has to be used to encrypt the challenge. This is when Net iD PIN-dialogue is shown (if not covered by Net iD SSO).
Card contents
Sjukvårdsrådgivningen
Jonas Öholm
9752 2688 857 0149 6686
2014-08-07
SITHS-kort
9752 2688 857 0179 9461
Certificates
Public Box
Private Box
Subject
For citizen e-services
Healthcare certificates
Optional for internal use
Root certificate
Cherry SmartBoard XX...
OMNIKEY CardMan 4321 0
RICOH Company, Ltd. ...
Net iD Components
SITHS CA v3, Carelink
Select a Certificate
Console Root
Certificates - Current User
Personal
Certificates
Issued To
Friendly Name
Jonas Öholm

Figur 4. SITHS kortet och ”MS-CAPI integration”.

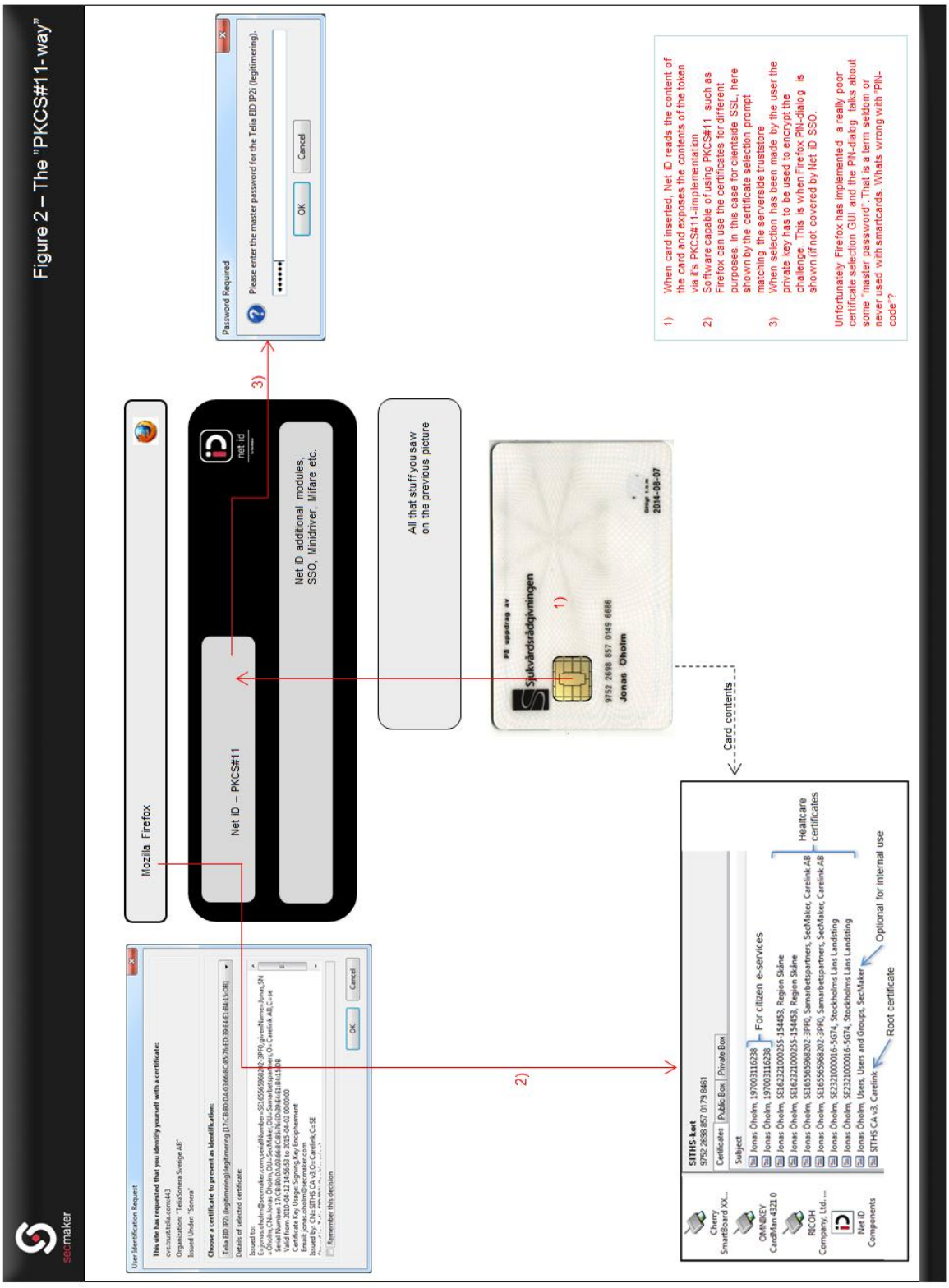
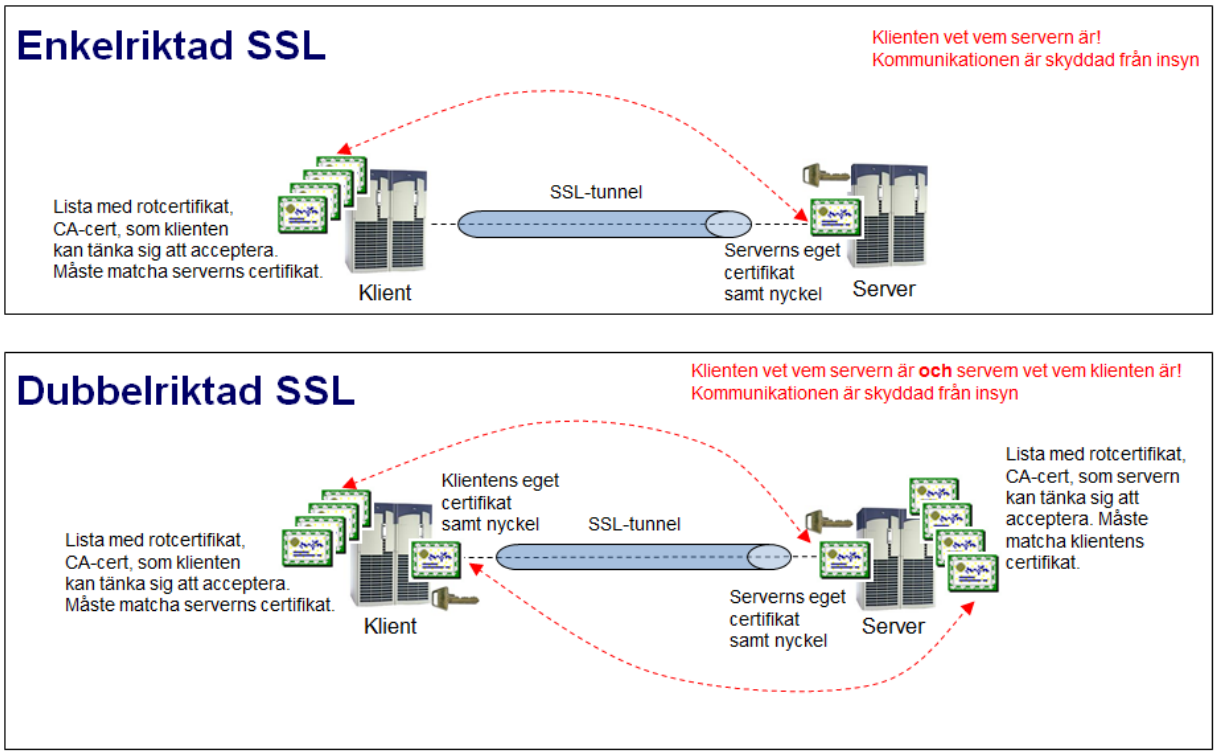


Figure 2 – The "PKCS#11-way"
secmaker
Mozilla Firefox
Net iD – PKCS#11
net id
Net iD additional modules, SSO, Minidriver, Mifare etc.
All that stuff you saw on the previous picture
Password Required
Please enter the master password for the Tela EID IP2i (legitimering).
OK
Cancel
1)
2)
3)
Sjukvårdsrådgivningen
9152 2698 857 0149 6686
Jonas Oholm
2014-08-07
Card contents
SITHS-kort
9752 2698 857 0179 8461
Certificates
Public Box
Private Box
Subject
For citizen e-services
Healthcare certificates
Optional for internal use
Root certificate
Cherry SmartBoard XX...
OMNIKEY CardMan 4321 0
RICOH Company, Ltd. ...
Net iD Components
1) When card inserted, Net iD reads the content of the card and exposes the contents of the token via it's PKCS#11-implementation
2) Software capable of using PKCS#11 such as Firefox can use the certificates for different purposes. In this case for clientside SSL, here shown by the certificate selection prompt matching the serverside truststore
3) When selection has been made by the user the private key has to be used to encrypt the challenge. This is when Firefox PIN-dialog is shown.(if not covered by Net iD SSO.
Unfortunately Firefox has implemented a really poor certificate selection GUI and the PIN-dialog talks about some "master password". That is a term seldom or never used with smartcards. Whats wrong with "PIN-code"?

Figur 5. SITHS kortet och ”PKCS#11 integration”.



Figur 6. Val av SSL-förbindelse.

Referenser

1. Guidelines for enabling smart card logon with third-party certification authorities http://support.microsoft.com/kb/281245
2. How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store http://support.microsoft.com/kb/295663/
3. Requirements for Domain Controller Certificates from a Third-Party CA http://support.microsoft.com/kb/291010/