Anvisningar för klientdator vid inloggning med certifikat på smarta kort

Revisionshistorik		
Version	Författare	Kommentar
0.1	Christoffer Johansson	Grundläggande dokument
0.2	Christoffer Johansson	Rättningar efter kommentarer från SecMaker, Inera och Certezza. Samt tempusbyte i Bakgrunden då många av problemen kvarstår.
0.8	Björn Skeppner	Infogat innehållsförteckning
0.9A	Christoffer Johansson	Tillägg av punkter om att klienten måste lita på utfärdaren av servercertifikat
1.0	Björn Skeppner	Justerat efter remisskommentarer

Innehåll

Målgrupp

Målgruppen för detta dokument är förvaltare av e-tjänster som samverkar i en SAML SSO-miljö. Primärt för Inera's e-Tjänster som samverkar med Säkerhetstjänsternas SSO-miljö.

Lämpligen bör detta dokument kunna utgöra grund/underlag till en generell anvisning som Inera's e-Tjänster kan kommunicera ut till de verksamheter som nyttjar e-Tjänsterna.

Bakgrund

Detta dokument är ett av tre dokument som levereras såsom en leverans av uppdraget:
" Uppdrag - Hantering av säkerhetsaspekter vid inloggning med SITHS-kort" [R1] som i sin tur har sitt ursprung av de incidentrapporter *Inera-INC-22948* och *Inera-INC-22953* som inkom till Ineras servicedesk under september 2013 och resulterade i en rapport:
" Rapport Säkerhetsproblem - SSO 2013-09-12" [R2].

De två andra dokumenten som uppdraget levererar är:

- Anvisningar för e-Arbetsplats som används vid inloggning med smarta kort/certifikat [R3]
- Anvisningar för användare vid användandet av e-Tjänster [R4]

Uppdraget skall således hantera anvisningar & krav på följande delar:

- e-Arbetsplatsen –användarens arbetsstation
- e-Tjänsten –den applikation som användaren nyttjar
- Användarens ansvar och skyldigheter

Eftersom användarhanteringen sker på flera olika nivåer i IT-arkitekturen, måste den också ses över på vart och ett av dessa ställen. De nivåer som identifierats och där brister förekommer är:

- **e-Arbetsplatsen**
  - Dålig information om de avgränsningar och begränsningar som finns för att hantera användarnas sessioner med hjälp av Net iD och SITHS-kortet. På sin höjd kan man avsluta SSL-sessioner mellan e-Arbetsplats och e-Tjänst, men e-Tjänstens applikationssessioner måste hanteras annorlunda.
  - Ofta är de e-Arbetsplatser och den miljö man befinner sig i inte testad. Därtill är inte e-Arbetsplatserna konfigurerade på ett optimalt sätt för att webbläsaren ska stängas ner och SSL-sessionen avslutas när SITHS-kortet avlägsnas.
  - Här ska tilläggas att dessa tester måste göras i varje unik miljö eftersom den är beroende av så många variabler och att användning av denna funktionalitet sker på eget ansvar.

- **e-Tjänsten/SP (Service Provider)**
  - Vissa e-Tjänster (SP) förväntar sig att SSL-sessioner som avslutas från e-Arbetsplatssidan innebär en utloggning från själva applikationen. Detta är dock inte sant och även om e-Arbetsplatsen lyckas stänga SSL-sessionen så handlar det om sessioner på olika nivåer som måste hanteras.
  - Det finns också variationer i hur SSL sessioner byggs och hanteras för olika e-Tjänster .
  - Avsaknad av riktlinjer för hur en e-Tjänst skall hantera sessioner däribland in- och utloggning av användare.
- **Användaren**
  - Utöver de brister i sessionshantering som kort beskrivs ovan identifierades också ett behov av information om det ansvar sjukvårdspersonalen har enligt PDL vad gäller hantering av personuppgifter i ett IT-system. I samband med att de tekniska möjligheterna förändras krävs en informationsinsats.

Syfte

Syftet är att på en övergripande nivå beskriva problemet på e-Arbetsplatsnivån i ovan bakgrund. Det vill säga:

- Vilka begräsningar e-Arbetsplatsen har och vilka avgränsningar som görs för detta dokument.
- Förutsättningar och krav på den IT-miljö/e-Arbetsplats där Net iD används för att möjliggöra att e-Arbetsplatser kan logga in med certifikat på smarta kort (SITHS-kort).
- Vilka förväntningar man kan ha då dessa certifikat används för logga in i tjänster/applikationer som ställer krav på inloggning med klientcertifikat.

Avgränsningar

Det som skrivs i detta dokument gäller inte så kallade ”egna paketeringar” av Net iD då dessa beställs enligt separat avtal mellan SecMaker och respektive organisation.

Detta dokument tar alltså bara hänsyn till de paketeringar av Net iD som distribueras via SITHS Förvaltning och som går under licensen *Net iD SITHS OEM Software.* Denna licens ger rätt till support på användning av Net iD vid kommunikation direkt från en e-Arbetsplats till en webbtjänst som kräver ett klientcertifikat vid inloggning.

Egna konfigurationer av Net iD som möjliggör uthoppslösningar och tunna klienter (ex. Citrix) har stöd i applikationen, men används under eget ansvar. Rekommendationen är att man upphandlar kompetens inom området, om den inte redan finns inom den egna organisationen.

Krav på e-Arbetsplatsen

Nedan följer de förutsättningar eller krav som finns på en e-Arbetsplats och IT-miljön den används i för att SITHS-kort och Net iD ska fungera som tänkt på arbetsstationen. Varje organisation måste själva kontrollera att deras e-Arbetsplatser följer dessa krav.

Net iD

Version

Inom SITHS används Net iD för att kunna läsa in certifikat från PKI-chippet på SITHS-korten och göra dessa användbara på e-Arbetsplatsen.

Vid händelser som kräver åtkomst till en användares privata nyckel ombeds användaren ange sin PIN-kod. Hur e-Arbetsplatsen kommunicerar med kortet via Net iD ser lite olika ut beroende på vilken webbläsare och vilket OS man använder.

Varje organisation måste säkerställa att den version av *Net iD SITHS OEM Software* som installeras på respektive maskin är godkänd för det OS och den/de Webbläsare som finns på maskinen. Supporterade versioner publiceras i *Release Notes* för Net iD, se följande referens (1).

Det finns också en matris som anger hur kritisk en uppgradering bedöms vara. De som klassas som Critical bör installera i organisationen så snart som möjligt eftersom de oftast åtgärdar någon form av säkerhetshål. Versioner med andra kategoriseringar kan vänta tills man hinner göra noggrannare tester i sin miljö. Denna matris återfinns här, (2)

Konfiguration

För att Net iD ska fungera som tänkt bör man också se till att göra viss enklare konfiguration av applikationen för anpassning till den egna IT-miljön. Detta bör göras i enlighet med den dokumentation som finns under följande referens (3) samt det som är aktuellt just för den release av Net iD som är används (4).

Två saker som ofta ställer till problem för Net iD är att:

- Man använder både Microsofts tjänst för Certifikatpropagering och den i Net iD. Microsofts tjänst kan lämpligtvis inaktiveras via Grupp principer, (5).
- Man använder fler än en Cryptographic Service Providers (CSP), ex. Bank ID och Net iD samtidigt. Dessa två fungerar inte bra tillsammans och det enklaste är att bara ha Net iD på de datorer som är i behov av att använda SITHS-kort. Om man måste köra flera CSP på en dator, så kan man på eget ansvar läsa mer här, (6).

OBS! Paketeringen av Net iD med SITHS OEM License har sin konfiguration i Windows registret som standard sedan det blev möjligt i version 6.0. Genom att inställningarna ligger i registret blir det enklare för IT-avdelningen att ändra parametrar i konfigurationen i efterhand via centrala administrationsverktyg som till exempel Grupp principer (Group Policys) i Microsoftmiljö.

Konfiguration av kortläsare

En annan viktig del för att SITHS-korten skall fungera på arbetsstationen är Kortläsaren. Det finns väldigt många olika modeller av kortläsare, men några punkter är viktiga att tänka på oavsett modell:

1. Se till att ha de senaste drivrutinerna från tillverkaren av den kortläsare som används. **OBS!** Det är inte rekommenderat att använda de drivrutiner som installeras automatiskt av Operativsystemet. Det är då bättre att vända sig till hemsidan för tillverkaren av dator/kortläsare alternativt SecMakers sammanställning över kortläsare, (7)
2. Energinställningarna på datorn är också viktiga att se över. Net iDs funktion **NetControl** tar bara bort certifikaten och stänger ner webbläsaren om den har kontakt med kortläsaren. Framförallt på bärbara datorer försätts kortläsaren i energisparläge när kortet rycks, vilket gör att Net iD tappar kontakten med kortläsaren.
3. Se över inställningarna för kortläsaren i BIOS, detta är extra viktigt om man har bärbara datorer eftersom vissa leverantörer redan i BIOS har inställningar som liknar dem i punkt 2 ovan.

För mer information kring konfiguration av kortläsaren se följande referens (8).

OS/Webbläsare

Detta är den del av miljön som kan vara svårast att kontrollera eftersom man vill installera uppdateringar från Leverantören av OS/Webbläsaren för att täppa till säkerhetshål samtidigt som dessa ibland kan ha oförutsedd inverkan på organisationens IT-miljö.

Det ska dock tilläggas att förändringar i dessa komponenter inte hittills har påverkat det som beskrivs under avsnittet **Förväntningar** nedan utan oftast har det haft inverkan på några av de **Utökade funktioner** som finns i Net iD och som beskrivs längre ner i detta dokument.

Vilka versioner av OS/Webbläsare som stöds i respektive release av Net iD hittas i Net iD Release Notes (1).

I övrigt har varje browser lite olika förutsättningar när det kommer till hantering av klientcertifikat på smarta kort. SecMaker, leverantören av Net iD, skriver lite om dessa på följande sida i referenslistan, (9).

Det ska också tilläggas att varje e-Tjänst i sig kan ha sina egna rekommendationer vad gäller e-Arbetsplatsen OS och Webbläsare. För information om denna typ av krav hänvisar vi till respektive e-Tjänst.

Tillit till SITHS CA[1] och åtkomst till dess distributionsplatser

Inom e-hälsa används ofta SITHS-certifikat både på e-Arbetsplatsen och på serversidan. För att användaren inte ska få upp varningar om att serverns certifikat inte är betrott måste e-Arbetsplatsen lita på utfärdaren av e-Tjänstens certifikat. Inom SITHS beskrivs detta mer utförligt i dokumentet **Teknisk beskrivning av SITHS Root CA v1** som återfinns på www.inera.se.

Ytterligare en funktion inom SITHS som är viktig för att allt ska fungera är att alla e-Arbetsplatser och servrar som använder SITHS har tillgång till följande funktioner:

- Revokeringstjänsten – används för att kontrollera om ett certifikat är giltigt eller revokerat.
- AIA-länkar – Används för att bygga en ”Chain of Trust” och alltså bygga för bygga tillit till alla servrar i kedjan av certifikatservrar inom en CA som SITHS. SITHS använder sig av något som kallas Authority Information Access (AIA-länkar) i certifikaten för att åstadkomma detta.

Om din organisation har en brandvägg som blockerar kommunikation med HTTP protokollet över TCP port 80 (vanlig webbtrafik) ut mot Sjunet/Internet måste det beställas brandväggsöppningar i enlighet med dokumentet Teknisk Beskrivning Root CA som hittas under SITHS tekniska dokument på www.inera.se. Detta dokument pekar ut sökvägarna (DNS-namnen) och IP-adresserna till ovan funktioner

Grundläggande funktioner

Om ovan krav uppfylls kan man förvänta sig att det fungerar att logga in mot de tjänster och webbtjänster som kräver ett SITHS klientcertifikat vid inloggning.

Det vill säga att Net iD klarar av att läsa SITHS-kortet och importera certifikaten till datorn. Dessa kan sedan användas av användaren vid inloggning till tjänster som kräver ett klientcertifikat utfärdat från SITHS.

Net iD ska också, om kraven uppfylls, klara av att ta bort certifikaten från datorn när kortet rycks. Detta förutsätter dock en riktigt konfigurerad e-Arbetsplats. Om certifikaten skulle bli kvar i datorn kan de dock inte användas vid en omförhandling av SSL-sessionen eftersom den privata nyckeln, som aldrig lämnar kortet, har avlägsnats. Dock kan en befintlig SSL-session fortgå tills den omförhandlas

Implementationer med tunna klienter och uthoppslösningar har stöd i Net iD men varje uppsättning är unik och omfattas inte av det nationella supportavtalet för Net iD. Detta och andra **utökade funktioner** beskrivs längre ner i detta dokument.

[1] CA – Certification Authority, begrepp inom Certifikatvärlden som kort beskriver avser organisationen och de system som är ansvarig för utgivningen av certifikat.

Utökade funktioner

Net iD kan förpaktereras med en viss konfiguration som aktiverar eller inaktiverar vissa utökade funktioner. Net iD med SITHS OEM License kommer förpaketerat med vissa utökade funktioner. Några av dessa diskuteras nedan men för att bli fullt insatt i vilken funktionalitet som är aktiverad bör man kontrollera konfigurationen i den Net iD man har installerad i sin egen miljö gentemot motsvarande dokument på följande referens, (3).

Om man följer kraven på e-Arbetsplatsen kan man också förvänta sig att det ska finnas kompatibilitet med de utökade funktioner som listas nedan och även andra ej aktiverade inställningar. Dessa används dock under respektive organisations eget ansvar.

Observera
Nedan angivna funktioner är ett urval av utökade funktioner som finns i Net iD, vissa av dem är aktiverade som standard i Net iD paketeringen med SITHS OEM License. Dessa ska dock betraktas som extra funktionalitet och ansvaret för test och användning av dem ligger alltså på respektive organisation.

Vid användning av dessa funktioner kan förändringar i Webbläsare eller OS resultera i att man måste göra ändringar i sina e-Tjänster eller IT-miljö för att bibehålla den utökade funktionaliteten.

Det är därför extra viktigt att ha en central kontroll över uppdateringar av OS/Webbläsare om någon av nedan funktioner används. Samt att göra egna tester om man är beroende av någon av dessa funktioner.

NetControl - Nedstängning av webbläsare när kortet avlägsnas

Tyvärr har man i vissa fall felaktigt kommit att använda utdragning av SITHS-kort som en godkänd metod för utloggning.

Nedstängning av webbläsaren med hjälp av Net iD's NetControl är dock inte att betrakta som en utloggning utan som en utökad funktion som egentligen bara innebär att webbläsaren/fliken stängs ned när smartkortet avlägsnas från kortläsaren.

NetControl fungerar så att ett programs ProcessID (PID), registreras (oftast en webbläsares eller webbläsarfliks PID) när en dubbelriktad SSL-session upprättas med hjälp av kortet. Dessa registrerade process ID:n kan sedan avslutas när kortet rycks, vilket för användaren kan verka som en utloggning fast det egentligen bara är webbläsaren/fliken som stängs ner och om allt går bra, även att den krypterade tunneln/SSL-sessionen avslutas på e-Arbetsplatsen. Den blir dock kvar på serversidan om man inte hanterar sessionens livslängd där.

En användare borde dock aldrig lita på att en nedstängd webbläsare är lika med en utloggning. I synnerhet inte i och med att browsertillverkare i allt högre grad försöker lagra så mycket information som möjligt om en e-Arbetsplats aktiva sessioner för att användaren skall kunna återta dessa vid eventuella krascher.

En användare inom svensk hälso- och sjukvård kommer alltid att vara ansvarig för att handlingar som innehåller patientinformation inte kan nås av en annan person efter det att man

själv är klar med handlingen. Oavsett om handlingen i sig är i fysisk (ex. pappersjournal) eller om den är digitalt lagrad och nås via ett Vårdsystem eller liknande.

Observera alltså att denna funktion inte är en fullständig utloggning ur en applikation, samt att ansvaret för användningen ligger på respektive organisation.

Som ett exempel så görs de tester som utförs för Nationella tjänster med specifika versioner av Net iD på korrekt konfigurerade e-Arbetsplatser. Detta för att visa att funktionen går att utnyttja, dock inte för att logga ut ur själva e-Tjänsten.

Följande sida i referenslistan kan användas som en guide för vad man bör tänka på om man trots allt väljer att utnyttja NetControl (8).

Net iD Plugin

Net iD har också ett pluginprogram som kan användas för att en webbtjänst ska kunna kommunicera med e-Arbetsplatsen och exempelvis visa information om kortet och vad som finns på det, men också anropa andra program och funktioner i Net iD.

För information om hur man kan använda pluginen bör man beställa Net iD Developer's Guide från SecMaker. Se också den tekniska beskrivningen av Net iD för att konfigurera de e-Arbetsplatser som skall logga in mot en sådan tjänst (3).

Vi rekommenderar dock inte att man bygger webbtjänstens funktionalitet gentemot pluginen eftersom detta skapar beroenden som är svåra att kontrollera. Hur pluginen ska laddas och vilka funktioner som finns är starkt kopplat till versioner av både OS/Webbläsare samt version av Net iD och konfiguration på e-Arbetsplatserna. Detta är faktorer som kan ändras utan att e-Tjänstens ägare vet om det och alltså påverka användarens upplevelse av tjänsten.

PIN-cache

Net iD har en funktion för att för att komma ihåg användarens PIN-kod. Detta ger en känsla av att man bara behöver logga in en gång, även om e-Arbetsplatsen gör inloggningar flera gånger i bakgrunden. Har man dessutom bara ett certifikatpar (Autentisering/Signering) på sitt SITHS-kort får man inte heller upp dialogen om att välja certifikat, vilket gör detta ännu mer osynligt. Konfigurationsparametern **ClearUserPinCache** kan användas för att kontrollera detta beteende. I skrivande stund är standardinställningen i Net iD med SITHS OEM License att denna cache rensas när kortet avlägsnas.

Inloggning på e-Arbetsplatsen

De nationella paketeringarna av Net iD har stöd för inloggning med smarta kort både på vanliga arbetsstationer och på tunna e-Arbetsplatser. Att de stödjer det innebär dock inte att allt kommer att fungera bara för att man installerar applikationen på server och e-Arbetsplats.

En felkonfigurerad lösning kan påverka både säkerheten och användarnas upplevelse. Varje implementation av inloggning med smarta kort på arbetsstationer är i någon mån unik. Detta gör

att support för denna form av lösning inte ingår i den nationella licensen. Vill man utnyttja denna typ av funktionalitet rekommenderar Inera att respektive organisation anlitar kompetens för om man inte redan har den inom organisationen.

SecMaker är en av leverantörerna som kan bistå med tjänster inom området och kan anlitas via avrop på ramavtalet som finns med Inera.

Net iD konfiguration & teknisk beskrivning

Även andra avancerade konfigurationer av Net iD kan göras för att modifiera hur applikationen fungerar. Dessa används också under eget ansvar och bör göras i enlighet med den tekniska beskrivningen för Net iD Enterprise, (3).

När man beställer en paketering av Net iD kan man från och med version 6.0 välja om konfiguration ska ske i en .config fil eller i datorns register (på Windows datorer).

OBS! Paketeringen av Net iD med SITHS OEM License använder konfiguration i Windows registret som standard. Genom att inställningarna ligger i registret blir det enklare för IT-avdelningen att ändra parametrar i konfigurationen i efterhand via centrala administrationsverktyg som till exempel gruppprinciper (Group Policys) i Microsoftmiljö.

Det går också att bygga egna MSI- paket (Microsoft Software Installation) för distribution med hjälp av gruppprinciper i Microsoftmiljö.

Checklista – inloggning med smarta kort

Kontrollera att din IT-miljö uppfyller följande:

☐ - Kontrollera att e-Arbetsplatsen litar på servercertifikat utfärdade från någon av SITHS CA-servrar. Mer information finns i dokumentet **Teknisk beskrivning av SITHS Root CA** på www.inera.se

☐ - Kontrollera att brandväggen är öppnad mot SITHS tjänster för revokeringskontroll och AIA-länkarna som specificeras i dokumentet **Teknisk beskrivning av SITHS Root CA** som återfinns på www.inera.se .

☐ - E-Arbetsplatsen använder en Net iD av så hög version som möjligt och som stödjs av e-Arbetsplatsens OS/Webbläsare, samt e-Tjänsten.

☐ - E-Arbetsplatsen har de senaste drivrutinerna från tillverkaren av kortläsaren

☐ - E-Arbetsplatsen inte försätter kortläsaren i strömsparläge när kortet avlägsnas, en inställning som kan göras både i BIOS och i Operativsystemet.

☐ - E-Arbetsplatsen inte använder både Microsofts Certifikatpropagering tillsammans med den i Net iD

☐ - E-Arbetsplatsen inte har fler än en CSP och då fördelaktigen bara Net iD om SITHS-kort skall användas.

☐ - E-Arbetsplatsen uppfyller de eventuella extra krav som ställs av respektive e-Tjänst som klientdatorerna ska logga in mot. Ex. krav på webbläsare, OS-version, patchnivå, Net iD version, att webbläsaren tillåter cookies, ev. scriptspråk etc.

☐ - Se över om konfigurationen i Net iD så att den passar er organisations krav.

☐ - Används några utökade funktioner i Net iD? Ex. Net iD plugin, NetControl, PIN-cache, användning i Citrixmiljö eller liknande? Observera då att ansvaret ligger på den egna organisationen för implementationen.

☐ - Är de olika klientlösningarna testade i den miljö de ska användas i och mot aktuella tjänster?

Referenslista

1. **SecMaker AB.** *Net iD - Release Notes.* [Online] https://service.secmaker.com/releasenotes/.

2. —. Net iD - Security Updates. [Online] https://service.secmaker.com/securityupdates/.

3. —. Net iD - Teknisk beskrivning **(kräver SITHS-kort)**. [Online] https://service.secmaker.com/secure/netidinfo/NetiD-Architectural_overview.aspx.

4. —. Net iD - Leveransinformation **(kräver SITHS-kort)**. [Online] https://service.secmaker.com/secure/siths/siths_leveransinformation.aspx.

5. —. Net iD - Stäng av MS Certifikatprograpagering (kräver SITHS-kort). [Online] https://service.secmaker.com/secure/netidinfo/Certificate_Propagation.aspx.

6. —. Net iD - Flera CSP på en dator **(kräver SITHS-kort)**. [Online] https://service.secmaker.com/secure/netidinfo/netidbankid2.aspx.

7. —. Kortläsare - Lista över kortläsare och drivrutiner. [Online] https://service.secmaker.com/unprotected/cardreaders.aspx.

8. —. *Net iD - Konfiguration kortläsare.* [Online] http://service.secmaker.com/unprotected/cardremove.aspx.

9. —. *Browserns förutsättningar **(kräver SITHS-kort)**.* [Online] https://service.secmaker.com/secure/examples/Web_browsers.aspx.

Ref	Dokumentnamn	Dokument
R1	Uppdrag - Hantering av säkerhetsaspekter vid inloggning med SITHS-kort	URL
R2	Rapport Säkerhetsproblem - SSO 2013-09-12	URL
R3	Anvisningar för klientdator som används vid inloggning med smarta kort/certifikat	URL
R4	Anvisningar för användare vid användandet av e-Tjänster	URL