Teknisk anslutning Pascal

Innehållsförteckning

TEKNISK ANSLUTNING PASCAL

1. Inledning

Vid inloggning till Pascal används som grund ett utgivet SITHS-kort för att unikt identifiera användaren. Behörighetskontroll och rättighetstilldelning sker med data från HSA-katalogen och Ineras Säkerhetstjänsters autentiseringstjänst (IdP). Verksamheter som ska använda Pascal måste därför se över systemkrav och rekommendationer, ett antal definitioner och implementeringen av desamma.

2. Olika inloggningssätt i Pascal

Pascal har tekniskt möjliggjort 3 olika inloggningssätt för användare:

1. Inloggning med **SITHS-kort** eller **SITHS eID-kort** med kortläsare via **NET iD-klient** kortläsarprogramvara
   Se kap 3
2. **SITHS eID-kort** med kortläsare via **SITHS eID Windowsklient** kortläsarprogramvara
   Se kap 4
3. **SITHS eID** via **SITHS eID Mobilklient** (på samma enhet eller på annan enhet)
   Se kap 5

3. Inloggning med SITHS-kort eller SITHS eID-kort med kortläsare via NET iD-klient kortläsarprogramvara

3.1. Operativsystem, webbläsare och Net iD

OBS!
Net iD-stödet efter 2023-06-30
Inera kommer sluta att tillhandahålla support för Net iD Enterprise i samband med att Ineras nuvarande avtal löper ut 2023-06-30. Viktigt att notera är att Inera efter 2023-06-30 ej kan säkerställa att SITHS eID-app för Windows kan samexistera med Net iD Enterprise.
Överväg därför SITHS eID och inloggningssätten 2 och 3 ovan

För att säkerställa att Pascals säkerhetslösning fungerar på ett korrekt sätt, bl.a. så att in- och utloggning fungerar, och att din webbläsare stängs när SITHS-kortet tas ur kortläsaren behövs följande systemkrav beaktas.

Följande kombinationer (OK) av operativsystem, webbläsare och Net iD stöds och supportas av Inera och Secmaker. Javascript och Cookies ska vara påslaget (enable) i webbläsarna nedan.

Operativsystem och webbläsare	Net iD	
	6.7.x och äldre	6.8.x
Windows 10		
IE 11 (32 bit)	ESK	OK**
Chrome	ESK	OK**
Edge/Chromium	ESK	OK**
Windows 8.1 Modern UI * **	**Paketering: SITHS1901*** **	
IE 11 (32 bit)	ESK	OK**
Chrome	ESK	OK**
Edge/Chromium	ESK	OK**

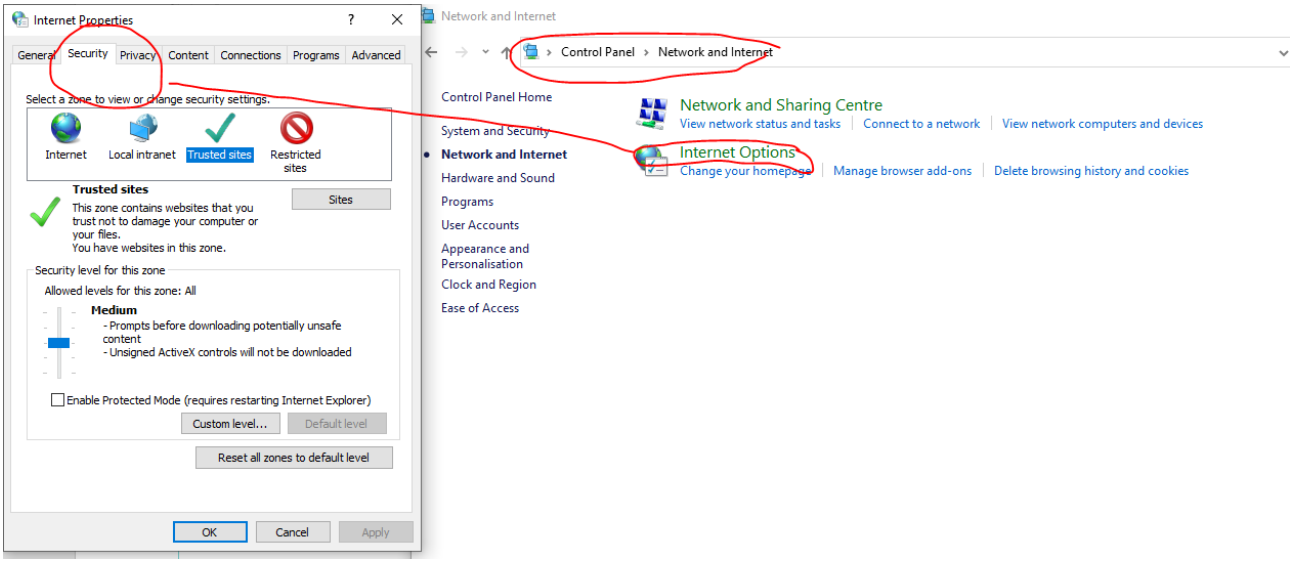
ESK = Inget stöd för denna kombination
OK = Stöd finns

** **OBS!** Paketering SITHS1301 måste användas. Tänk på att denna paketering inte stödjer utloggning ur Pascal via utdragning av SITHS-kortet. Därför ska man alltid använda knappen **Logga ut** i Pascal vid utloggning, vilket är den primära utloggning som alltid bör användas.

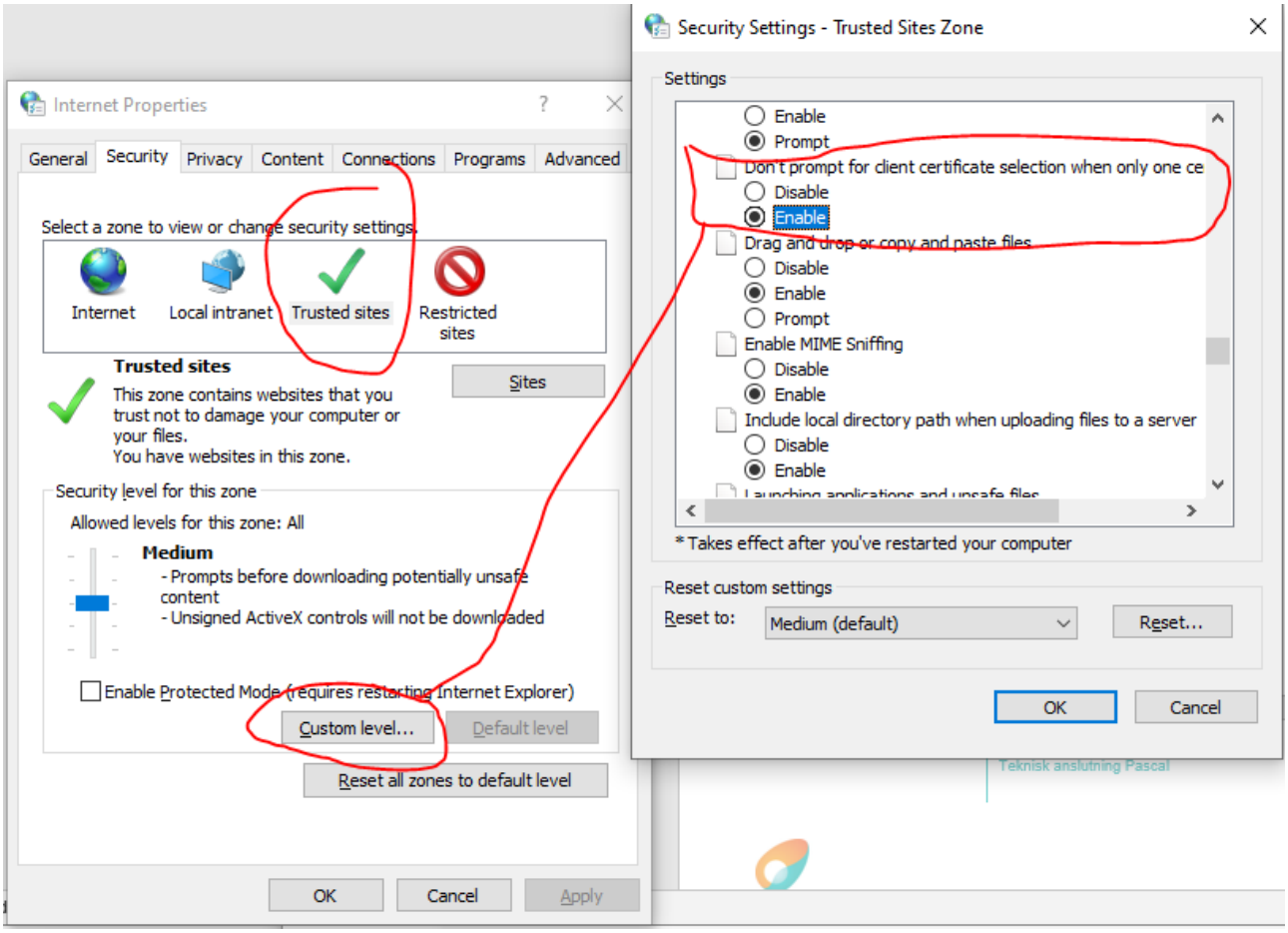
*** **OBS!!** Modern UI är det läge/användargränssnitt som introducerades i och med lanseringen av Windows 8. Modern UI är standardgränssnittet i Windows 8.1 och är speciellt anpassat för mobila enheter t ex. surfplattor. Observera att det då är paketering **SITHS1901** som ska användas.

Andra kombinationer än ovan kan fungera men stöds och supporteras inte av Inera & Secmaker. Om man har en annan kombination så ska man testa så att in- och utloggning sker på ett korrekt sätt. Om så inte sker ska man uppdatera sin konfiguration enligt matrisen ovan.

Vi rekommenderar att man markerar i webbläsarens inställningar att vid inloggning visa certifikat endast då fler än ett certifikat finns på SITHS-kortet. Detta sker enligt följande:



Välj – fliken **Säkerhet** – markera **Betrodda platser** och klicka på knappen **Anpassad nivå i Kontrollpanelen**. Markera **Aktivera** under rubriken ”Fråga inte efter val av klientcertifikat när det bara finns ett certifikat”

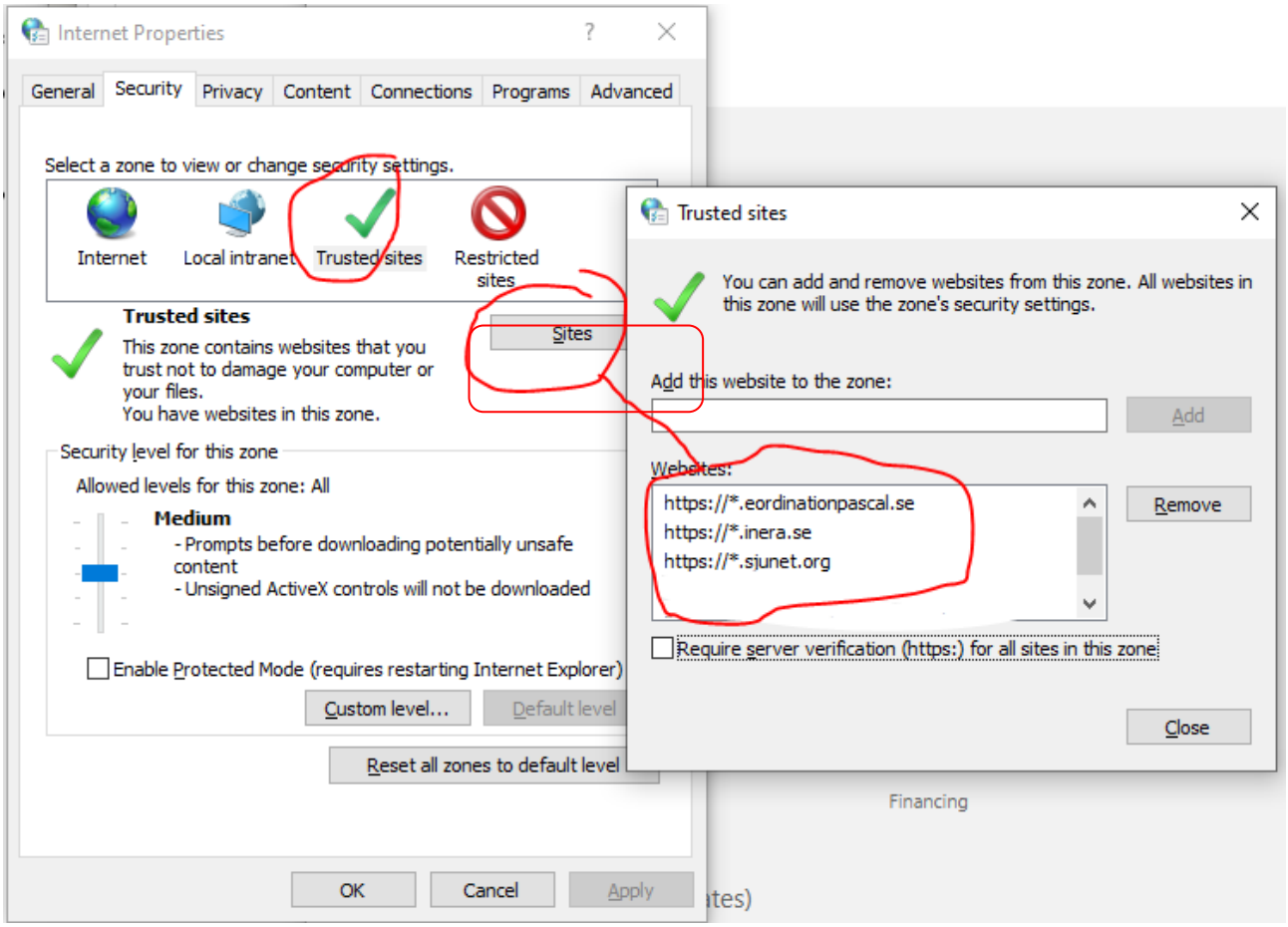


Anpassa säkerhetsnivån i webbläsaren

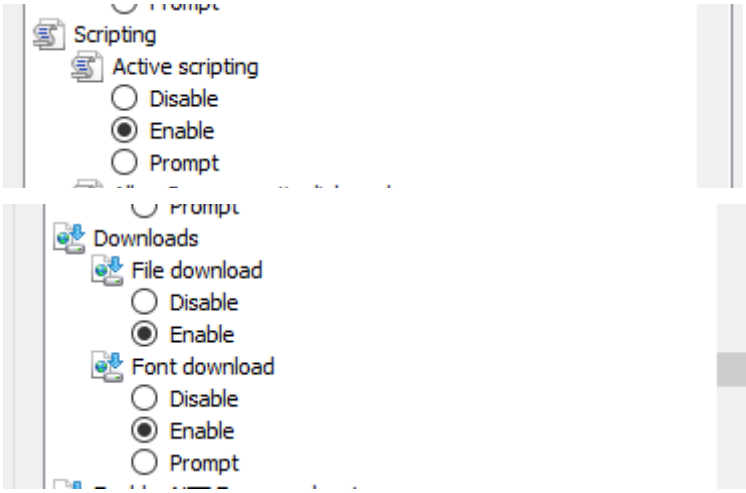
För att SITHS-korthantering och SingleSignOn ska fungera som tänkt, ska aktuella domäner/siter som säker inloggning sker mot finnas inlagda som "Betrodda platser" i Kontrollpanelen.

Lägg till följande domäner under fliken **Säkerhet** – **Betrodda platser** - **Platser** i Windows kontrollpanel:

- https://*.eordinationpascal.se
- https://*.inera.se
- https://*.sjunet.org



Säkerhetsnivån skall vara mellan. Man kan ändra säkerhetsnivån, men inte parametrarna ”Active scripting”, ”File download” och ”Font download” som måste vara satta till Enable.



3.2. Net iD (kortläsarprogramvara)

Vi stödjer Net iD version enligt matris ovan.

Om organisationen har en direktanslutning till SITHS (har avtal med Inera) så finns det på SITHS projektplats installationspaket att ladda ner som innehåller rätt inställningar i Net iD (enbart RA-organisationen, Registration Authority har tillgång till detta). Är man ansluten till SITHS via en annan organisation (tredjepartanslutning), så kan denna organisation tillhandahålla installationspaket för Net iD.

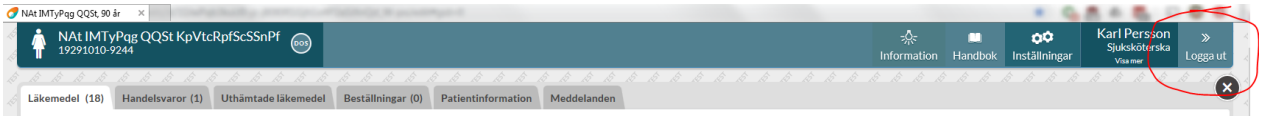
I vissa fall kan man ha gjort lokala anpassningar av Net iD. Den information (beroende på version av NetId) som behöver finnas i Windows registry alternativt i konfigurationsfilen (iid.cfg) under program/Net iD för att Net iD:s nedstängning av webbläsaren ska fungera är:

Namn	Typ	Data
(Standard)	REG_SZ	(värde har ej angetts)
Applications	REG_SZ	iexplore.exe;firefox.exe;chrome.exe
Ask	REG_SZ	0
Enable	REG_SZ	1
LogonApplications	REG_SZ	iexplore.exe;firefox.exe;chrome.exe
TabNames	REG_SZ	TabWindowClass;MozillaUIWindowClass;MozillaWindow...

```
[NetControl]
Applications=iexplore.exe; iidxweb.exe
Ask=0
Enable=1
```

Det kan finnas andra sätt att få nedstängning av webbläsaren att fungera än som beskrivits ovan, men då får man själv genomföra tester så att nedstängning av sessionen sker på ett korrekt sätt när SITHS-kortet rycks ur kortläsaren.

Det är dock viktigt att understryka att den primära utloggningen ur Pascal är att alltid använda knappen Logga ut. (se bild)



Ibland kan man vid inloggning få upp en lång lista med certifikat, vilket bl. a kan ske om arbetsstationen används av flera användare. Detta kan upplevas som irriterande när man måste leta i listan för att hitta sitt certifikat. I Net iD har alltid funktionen ”CertMover” funnits. Funktionen läser in kortets användarcertifikat och lägger dem åtkomliga för t.ex Internet Explorer. ’CertMover’ är helt enkelt "det som snurrar" i taskbar när du stoppar i ett kort. Windows har en egen sådan funktion som via Net iD:s CSP ber om samma operation. Det kan då ibland uppstå oönskade fenomen såsom att det blir certifikat liggande kvar i MyStore. På Secmakers servicesida finns det en beskrivning för hur man kan få bort detta, se följande länkar (man måste autentisera sig med sitt SITHS-kort för att få åtkomst):

https://service.secmaker.com/secure/netidinfo/Certificate_Propagation.aspx
https://service.secmaker.com/secure/examples/smartcard_gpo.aspx

Stora IT-lösningar har ofta komplexa samband och registerändringar och stopp av tjänster kan ge oväntade resultat. Prova med försiktighet och helst i en testmiljö innan du aktiverar ändringen i produktionsmiljö.

4. Inloggning med SITHS eID-kort med kortläsare via SITHS eID Windowsklient kortläsarprogramvara

Se https://confluence.cgiostersund.se/pages/viewpage.action?pageId=220213869

5. Inloggning med SITHS eID via SITHS eID Mobilklient (på samma enhet eller på annan enhet)

Se https://confluence.cgiostersund.se/pages/viewpage.action?pageId=220213869

6. Brandväggar

För att komma åt Pascal krävs att följande brandväggar är öppna, se nedan.

Sjunet

IP-adress	Url	Port
81.89.154.161	https://siths.eordinationpascal.sjunet.org	443
82.136.182.2	https://idp.inera.se	443
81.89.154.161	https://eid.eordinationpascal.sjunet.org	443

Internet

IP-adress	Url	Port
164.40.178.0	https://siths.eordinationpascal.se	443
82.136.182.2	https://idp.inera.se	443
164.40.178.0	https://eid.eordinationpascal.se	443

OBS! Kontrollera att adressen ovan inte spärras i någon generell produkt för internetfiltrering.

IdP (Identity Provider) är tillgänglig på både Sjunet och Internet med samma hostname. Detta hostname resolvar olika IP-adresser beroende på vilket nät/DNS som används. Inera IdP är tillgänglig från både Internet och Sjunet med samma instans och domän. De IP-adresser som används av tjänsten finns i en range som länge funnits endast på Sjunet så i många fall kan brandväggar (443) behöva öppnas mot angivna adresser för de klienter på nätverk som ska nå Pascal. Det beror på hur er organisation med klienterna routar 82.136.182.0/24 nätet.
Organisationer med både internet- och sjunetanslutning behöver för en fullständig anslutning över Sjunet - för både DNS-uppslag och IdP-trafik - ett extra steg.
För klienter som har DNS-uppslag för både sjunet och internetdomäner adderas en s.k. Conditional Forward i den DNS lösning som används av er idag (som troligen redan har en sådan för sjunet.org).
Utan detta finns risk att trafik mot IdPn går över internet när anslutningen är tänkt att vara över Sjunet, och detta kan t ex uppmärksammas först när internetanslutningen får problem. Förslagsvis valideras vägvalen som går från klient mot respektive miljö med tracert och/eller nslookup. Vid validering kan en rensning av eventuell DNS cache behövas (”ipconfig /flushdns” på Windows).

Dessutom behövs följande **revokeringsadresser** (för kontroll av indragna/ogiltiga certifikat) vara öppna:

CAv1

För att komma åt nya spärrar/AIA-lokationer så får följande adresser inte vara blockerade:

Internet:
http://ocsp1.siths.se (IP 82.136.183.247 och 194.237.208.174)
http://aia.siths.se (IP 82.136.183.248 och 194.237.208.239)
http://crl1.siths.se (IP 82.136.183.246 och 194.237.208.239)
Port 80
Sjunet:
http://ocsp2.siths.sjunet.org (IP 82.136.160.42)
http://aia.siths.sjunet.org (IP 82.136.160.44)
http://crl2.siths.sjunet.org (IP 82.136.160.44)
Port 80

Brandväggar måste också öppnas för att HSA- och SITHS-organisationen ska komma åt HSA Admin och SITHS Admin men det tas inte upp i detta dokument.

Detta görs av nätverkstekniker i samband med tjänsternas införande.

7. Kortläsare och drivrutin

Vissa kortläsare med dess drivrutin kan ibland inte registrera att SITHS-kortet har ryckts ur kortläsaren. Det innebär att Net iD inte upptäcker att något har hänt och följaktligen inte stänger ner sessionen.

Vi rekommenderar därför att ni utgår från Secmakers kortläsarbroschyr, som innehåller kortläsare som fungerar bra. Det är också viktigt att man använder den senaste drivrutinsversionen från tillverkaren. Använd **inte** Microsofts generiska drivrutiner.

Andra läsare kan också fungera bra men var noga med dess drivrutiner.

I båda dessa fall så bör man testa så att kortläsaren och dess drivrutin fungerar korrekt, se stycket om funktionstest av SITHS-kort och dess kortläsare nedan.

När man installerar drivrutiner för olika kortläsare uppmärksammar man sällan att vissa installeras med **strömspar PÅ** medan andra installeras med **strömspar AV**. Det har visat sig att strömsparfunktionen kan ställa till med en del märkliga bieffekter i applikationer som pollar efter kort på ett visst sätt. **Ta därför för vana att stänga av strömsparfunktionen för kortläsaren om du får problem.**

8. Pdf-läsare

Utskrift av ”Förteckning recept” i Pascal fungerar med Adobe Reader version 9 eller senare. Tidigare versioner kan fungera men stöds inte av Inera och eHälsomyndigheten. Om man har en tidigare version än Adobe Reader 9 får man själv testa och validera att utskrift av ”Förteckning recept” sker på ett korrekt sätt.

9. Versioner av Net Id, dator och SITHS-kort och certifikat

Man kan själva få ut information om sin konfiguration genom att med SITHS-kort i kortläsaren gå från en dator med webbläsaren IE11 eller äldre versioner av Edge (ej Chromiumbaserade Edge) till adressen https://test.siths.se och se sin konfiguration.

10. Tunna klienter

För information och frågor gällande tunna klienter med **Net iD** gäller följande rekommendationer:

1. Kontrollera om supportavtal finns med leverantören/tillverkaren av plattformen.
2. Kontrollera om det finns eget avtal med Secmaker avseende Net iD.

   Om supportavtal finns enligt ovan, så vänd er i första hand till dessa för information och support.

3. Om man inte har några supportavtal eller får hjälp enligt ovan kan man via mail, vända sig till Inera support, support@inera.se, för hjälp och vidare rådgivning.

För information och frågor gällande tunna klienter (mobilklienter/tablets) med **SITHS eiD** gäller följande:

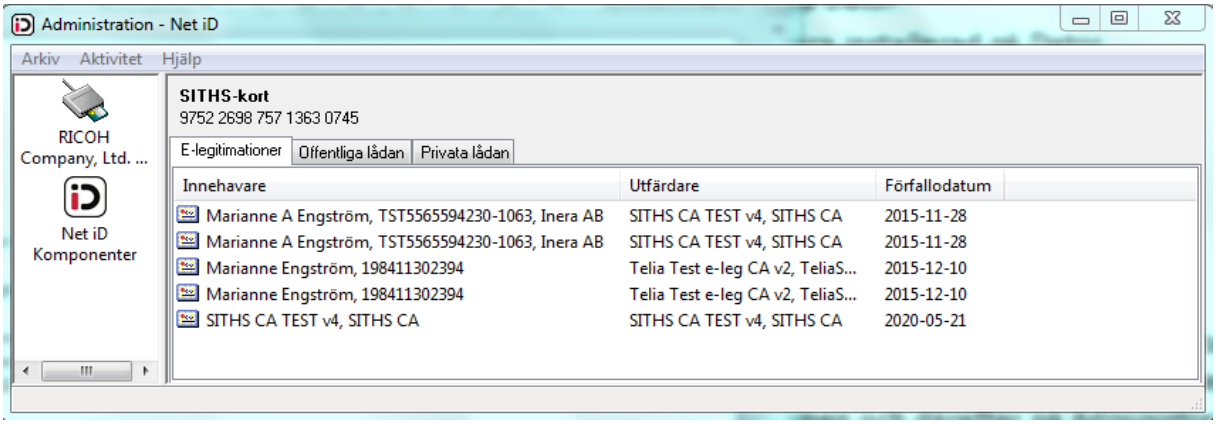
Se https://confluence.cgiostersund.se/pages/viewpage.action?pageId=220223026

11. Funktionstest av SITHS och kortläsare

Funktionstest av SITHS-kort och dess kortläsare kan ske på följande sätt:

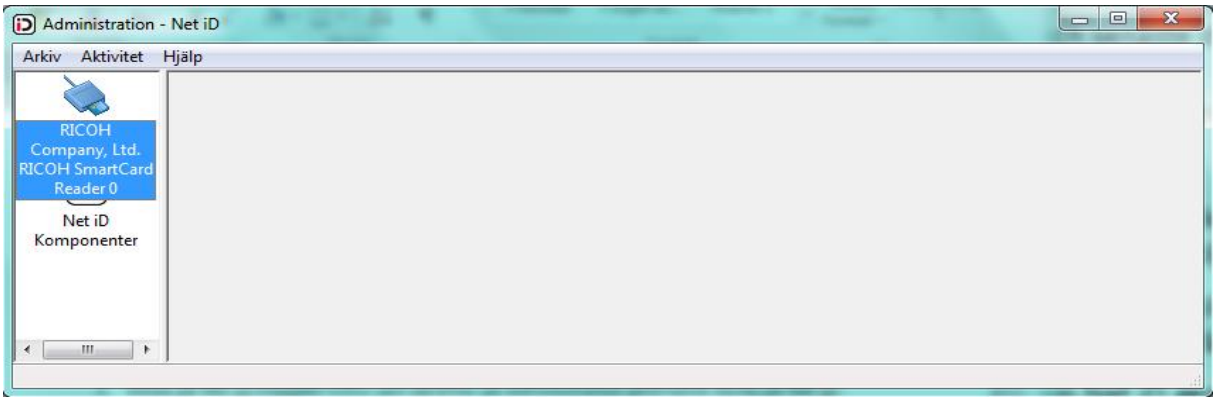
1. Anslut kortläsare till datorn och sätt i SITHS-kortet i kortläsaren.
2. Leta upp Net iD genom att klicka på **Start** och därefter **Alla Program**. Klicka på **Net iD-mappen** och därefter på **Administration** eller Högerklicka på **Net iD-ikonen** och därefter på **Administration** (gamla) om den finns på datorns skrivbord.

   Då visas ett Net iD-fönster där alla certifikat som finns på SITHS-kortet visas.



3. Ryck ur SITHS-kortet ur kortläsaren.

Då ska alla certifikat som finns på SITHS-kortet försvinna från Net iD-fönstret. Om så inte sker så är det fel på kortläsaren och/eller dess drivrutin.



4. Testa ditt SITHS-kort, certifikat och pinkoder på Ineras testsida.

12. Testa ditt SITHS eID

Testa ditt SITHS eID, certifikat och pinkoder på https://test.idp.inera.se/