



Direktoratet for
e-helse

Kjernejournal

Teknisk tilrettelegging for legekontor

Oppdatert 25.10.2016



Publikasjonens tittel:

Kjernejournal – Teknisk tilrettelegging
for legekantor

Utgitt:

25.10.2016

Utgitt av:

Direktoratet for e-helse

Kontakt:

postmottak@ehelse.no

Postadresse:

Postboks 6737 St. Olavs plass, 0130
OSLO

Besøksadresse:

Verkstedveien 1, 0277 Oslo
Tlf.: 21 49 50 70

Publikasjonen kan lastes ned på:

www.ehelse.no

Innhold

1 Om dette dokumentet	4
2 Framgangsmåte for tilrettelegging av kjernejournal på legekantor	4
Informasjon til teknisk tilrettelegger	5
Hjelpemidler fra Direktoratet for E-helse - "Miljøapp"	5
Oppgradere EPJ-system	6
Sertifikater	6
Virksomheten må ha et gyldig Virksomhetssertifikat	6
EPJ-systemet må kjenne til kjernejournalens virksomhetssertifikat	7
Virksomheten må stole på rot-sertifikatene til Buypass	7
Verifisere og eventuelt å oppgradere Java	8
Sjekk om Java er installert	8
Installere nyeste versjon av Java	9
Avinstallere gjeldene versjon av Java	9
Verifisere og eventuelt oppgradere nettleser	9
Åpne for kommunikasjon til kjernejournal	10
Tilkoblingssjekker (Buypass)	12
Riktig klokke på PC og server	13
Oppdatering av operativsystemer på PC og servere	14
Informasjon til brukerne	14
Sertifikater	15
Personlig sertifikat	15
Verifisere smartkort (Buypass)	15
Bruke eHelsebrukerportal for å sjekke personlig informasjon og ta godkjenningssprøve	16
Status Helsepersonellregisteret	16
Autorisasjon som helsepersonell	16
Kom i gang med kjernejournal	17
3 Vedlegg	18
Vedlegg 1: Problemløsning	18
Vedlegg 2: Risiko- og sårbarhetsanalyse	21
Vedlegg 3: Oversikt over nødvendige portåpninger for Kjernejournal	25

1 Om dette dokumentet

Dette er en steg-for-steg guide for å koble opp EPJ med kjernejournal fra et legekantor. Dokumentet beskriver kravene som må fylles, samt tester som bør kjøres for å verifisere at IT-miljøet er tilrettelagt for kjernejournal.

Det er anbefalt at kontoret har en person som er ansvarlig for å gjennomføre punktene i dette dokumentet. Den som vanligvis har ansvar for å tilrettelegge de tekniske løsningene ved kontoret, kan gjøre dette på en god måte. Et alternativ kan være at driftsleverandør gjør det.

Er det tekniske avklaringer eller spørsmål til kjernejournal, så rettes disse til:

- **Lokal IT / driftsleverandør** hvis det er utfordringer i egen teknisk infrastruktur (brannmuråpning, Java e.l.)
- **EPJ-leverandørens** supportapparat, hvis spørsmål / problemer i forbindelse med oppkobling mot kjernejournal (korrekt versjon av EPJ, sertifikathåndtering, aktivering av funksjonalitet i EPJ).

Tilbakemeldinger på selve dokumentasjonen kan sendes til: kjernejournal@ehelse.no

Se [Informasjon til Bruker](#) (side 15) for hva brukere av EPJ må gjøre for å få tilgang til kjernejournal. Begge må følges for å sikre vellykket integrasjon med kjernejournal.

2 Framgangsmåte for tilrettelegging av kjernejournal på legekantor

For at en bruker i et legekantor skal kunne koble seg på kjernejournal, er det en del forutsetninger som må være på plass. Dette gjelder både juridisk/avtalemessig, personlig informasjon, virksomhetens informasjon, samt teknisk integrasjon med kjernejournal fra lokalt fagsystem.

Dette dokumentet er en guide for å tydeliggjøre hvordan dette skal gjøres, samt noe tips til hvordan man kan verifisere oppsettet. Dersom man har ytterligere spørsmål kontaktes leverandør av virksomhetens EPJ-system

Informasjon til teknisk tilrettelegger

Følgende informasjon er for teknisk tilrettelegger for å klargjøre PC for bruk av kjernejournal.

Her er en kort oppsummering av hva som må på plass. Detaljer kommer nedover i dokumentet.

- Java må være installert for å kunne logge på kjernejournal
 - Unntak: BuyPass tilbyr pålogging uten Java
- Sørge for at rett versjon av EPJ-systemet benyttes
- Sørge for at rett versjon av nettleser benyttes (avhengig av EPJ system)
- Aktivere kjernejournal i EPJ
- Virksomheten må ha virksomhets sertifikat fra Buypass eller Commfides, med korrekt organisasjonsnummer for virksomheten
- EPJ-systemet må kjenne til kjernejournal sitt signeringssertifikat
- Virksomheten må ha Buypass sitt rot-sertifikat installert som en trusted root
- Verifisere kommunikasjon til kjernejournal, Buypass eller Commfides

Hjelpemidler fra Direktoratet for E-helse - "Miljøapp"

Direktoratet for e-helse har laget en sjekk-mitt-miljø-applikasjon som kalles MiljøApp. Denne kan lastes ned og kjøres for å verifisere lokalt oppsett. Denne vil det henvises til flere steder i denne guiden. Applikasjonen kan lastes ned fra:

<https://ehelse.no/e-resept-kjernejournal-og-helsenorgeno/kjernejournal/teknisk-tilrettelegging-for-kjernejournal>

Denne vil da hjelpe med å sjekke følgende:

- at du har en fungerende versjon av Java
- at du har en fungerende versjon av nettleser
- at den kommunikasjonen til kjernejournal, Buypass og Commfides fungerer
- at virksomhets sertifikatet er i orden

Oppgradere EPJ-system

For å kunne ta i bruk kjernejournal, må legekontorets EPJ-system være oppgradert til en versjon som støtter kjernejournal. Hvordan oppgraderingen av EPJ-systemet skal skje/hvem som skal foreta oppgraderingen, avtales mellom den enkelte virksomhet og EPJ leverandør.

Leverandør	Journalssystem	Fra versjon
Infodoc	Plenario	2.20
Hove	SystemX	2013 R1 (4120)
CGM	WinMed2	2.16 R2 B5
CGM	CGM Journal	108
CGM	Vision	4.6
DIPS	DIPS	7.3.10
Siemens	Doculive	6.5.5 SP2
CSAM	Amis	2.46.4

Aktivering av kjernejournal må utføres i EPJ-systemet. Se brukerveiledning for EPJ-systemet eller ta kontakt med EPJ-leverandør. Selve aktiveringen av kjernejournal for hele legesenteret, eller for enkelte helsepersonell, utføres gjerne av den eller de personene som har et særskilt teknisk/administrativt ansvar for EPJ på kontoret. Dokumentasjon finnes på helsedirektoratet sine nettsider:

<https://ehelse.no/e-resept-kjernejournal-og-helsenorgeno/kjernejournal/teknisk-tilrettelegging-for-kjernejournal>

Sertifikater

Virksomheten må ha et gyldig Virksomhets sertifikat

Alle legekontor må ha virksomhets sertifikat (utstedes av Buypass eller Commfides).

NB!

Virksomhets sertifikatet benyttes til å identifisere virksomheten det gjøres oppslag fra. Dette loggføres i kjernejournal sammen med legens navn og HPR-nummer. Alle som har gjort oppslag vises for innbygger i deres kjernejournal på helsenorge.no. Det er derfor viktig at organisasjonsnummeret i virksomhets sertifikatet stemmer overens med det som er registrert i enhetsregisteret.

NB!

Sertifikatene må til en hver tid være gyldige, og rutiner for å sikre dette må være etablert og i bruk. Dersom ditt legekantors sertifikat utløper i løpet av de neste seks måneder, er det viktig at du bestiller et nytt.

De fleste legekantor lar sin EPJ-leverandør håndtere sertifikatene. Dersom du ikke er sikker på om sertifikatet er gyldig eller trenger å bestille nytt, ta kontakt med din EPJ-leverandør, eller driftsleverandør.

Bestilling av virksomhets sertifikat kan gjøres her:

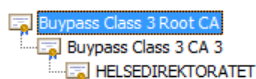
- Buypass: <https://www.buypass.no/produkter-og-tjenester/virksomhets sertifikat>
- Commfides: <https://www.commfides.com/e-ID/Bestill-Commfides-Virksomhets sertifikat.html>

EPJ-systemet må kjenne til kjernejournalens virksomhets sertifikat

Kjernejournal signerer meldinger som sendes til EPJ, så EPJ må derfor kjenne til kjernejournalens virksomhets sertifikat.

Kjernejournalens virksomhets sertifikat som benyttes til signering (keyUsage: non-repudiation) er **gyldig frem til 16. desember 2018**. Det kan finnes via NHNs adresseregister via herid 95324 eller via Buypass på serialnr 983544622 .

Virksomheten må stole på rot-sertifikatene til Buypass



Kjernejournal benytter sertifikater som er utstedt av Buypass. For å få koblet til kjernejournal må EPJ-systemet stole på Buypass sine rot-sertifikater. Dette er de samme som for eksempel e-resept og vil være tilgjengelig på din pc eller server. I de fleste tilfeller er dette på plass fra før.

Dersom rot-sertifikatene mangler, må disse sertifikatene legges inn under:

Local Computer / Trusted Root Certification Authorities / Certificates

Buypass Class 3 Root CA	http://www.buypass.no/cert/BPClass3RootCA.cer
Buypass Class 2 Root CA	http://www.buypass.no/cert/BPClass2RootCA.cer

Sertifikater kan administreres i Windows gjennom Certificate Manager ([certmgr.msc](#))

Commfides benytter et rot-sertifikat som er lagt inn i Windows ved installasjon, så det behøves ingen oppdatering for Commfides.

Verifisere og eventuelt å oppgradere Java

Hvis du ikke logger på den Javafrie løsningen til Buypass, krever kjernejournal at Java er installert for at du skal kunne logge på med enten Buypass- eller Commfides-smartkort.

For å teste dette kan man benytte vår MiljøApp som tar en test av ditt oppsett. Se kapittelet [Hjelpemidler fra Direktoratet for E-helse - "Miljøapp"](#) for detaljer.

Kjernejournal anbefaler å bruke Java 8 siste versjon. Hvis din Java-versjon er for gammel vil kjernejournal gi en advarsel om det. Det har vist seg at gamle Java-versjoner kan forårsake lang påloggingstid fordi de ikke leser proxy-innstillingene fra nettleser som er nødvendig for å nå Helsenettet. Da må Java-versjonen oppgraderes. Se også dette kapittelet: **Hvis lang påloggingstid.**

Sjekk om Java er installert

Hvis du ønsker å sjekke om du har Java installert på en maskin uten tilgang til internett:

1. Åpne «Kontrollpanel» fra startmenyen i Windows (eller under «Innstillinger - avhengig av Windows-versjon)
2. I Kontrollpanel, åpne "Programmer og Funksjoner" eller "Legg til / fjern programmer"
3. Her ser man en liste over installerte programmer.
 - a. Hvis Java ikke står der må dette installeres
 - b. Hvis du ikke har siste versjon, så bør Java oppdateres

Hvis du ønsker å sjekke om du har Java installert på en maskin med tilgang til internett:

1. Gå til følgende side i Internett Explorer:
<https://www.java.com/en/download/installed.jsp?detect=jre>
2. Hvis Java- appleten spør om lov til å kjøre, klikk for å godta det
3. Appleten viser resultatet av sjekken

Tips: Hvis du får startet MiljøApp-applikasjonen, så er Java installert

Installere nyeste versjon av Java

Dersom du har en gammel versjon av Java installert, avinstaller gammel versjon først. Se under.

For å installere nyeste versjon:

1. Gå inn på følgende internett side <http://www.java.com/en/download/manual.jsp>
2. Velg **Offline**-versjonen
3. Følg instruksene på websiden

Avinstallere gjeldene versjon av Java

Hvis Java ikke foretar en automatisk avinstallering av den gamle versjonen, bør du avinstallere selv:

1. Gå inn på **Kontrollpanel** og **Programmer og funksjoner**
2. Finn oppføringen **Java** (med påfølgende versjonsnummer, for eksempel "Java 7 Update 21") og dobbeltklikk på den.
3. Velg «Ja» når du blir spurt om du er sikker

Verifisere og eventuelt oppgradere nettleser

Kjernejournal krever en nyere versjon av Microsoft Internet Explorer (IE) for at informasjonen skal presenteres på en lesbar måte. Kravet er IE9, IE10, IE11 eller Chrome v33.

For å teste dette kan man benytte vår MiljøApp-applikasjon. Se kapittelet [Hjelpemidler fra Direktoratet for E-helse - "Miljøapp"](#) for detaljer.

DIPS har integrert Chrome v33 i sin løsning. Hvis legekantoret bruker DIPS, behøver du ikke sjekke om legekantoret har riktig nettleser

For å sjekke IE-versjon:

1. Åpne IE
2. Klikk **Hjelp** / **Verktøy** (Alt-X)
3. Velg **Om Internet Explorer**
4. Versjonsnavnet vises i dialogvindu

1.

NB!

Før en eventuell oppgradering, sjekk om legekantor har noen andre fagsystemer som benytter IE, og som krever eldre versjoner av IE. Hvis dere er usikre, ta kontakt med leverandøren av gitte fagsystem.

Direktoratet for e-helse anbefaler at man legger inn ***.kjernejournal.helsedirektoratet.no** som Trusted Sites / Klarerte Områder i IE.

Dette utføres på følgende måte:

1. Gå inn på «Alternativ for Internett»
2. Velg fanen «Sikkerhet»
3. Merk ikonet som heter «Klarerte områder»
4. Trykk på knappen «Områder»
5. Legg inn *.kjernejournal.helsedirektoratet.no Trykk Lukk, og deretter ok i «Alternativer for Internett»

Åpne for kommunikasjon til kjernejournal

For å få kontakt med kjernejournal må legekantoret være tilknyttet Helsenettet. For mer info om Helsenettet se <https://www.nhn.no/hjelp-og-brukerstotte/helsenettet/Sider/default.aspx>

For å teste dette kan man benytte vår MiljøApp-applikasjon. Se kapittelet [Hjelpemidler fra Direktoratet for E-helse - "Miljøapp"](#) for detaljer.

Hvordan konfigurere sikker Proxy for å validere signaturer

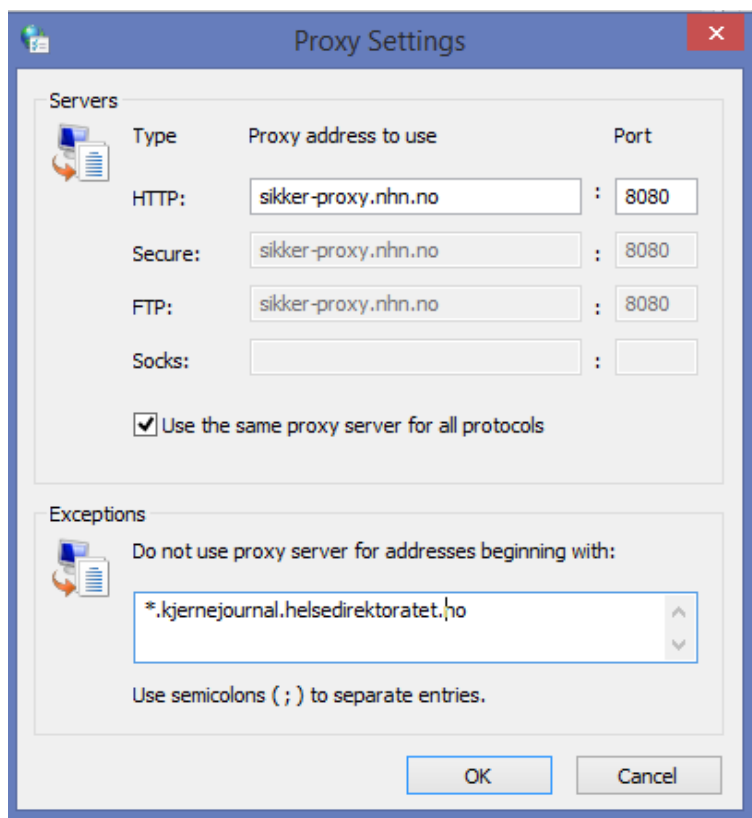
Når man bruker sikker proxy, vil EPJ-systemet ikke få kontakt med kjernejournal. Du må konfigurere slik at det lages unntak for de aktuelle kjernejournaladressene.

Forklaring: Applet fra både Buypass og Commfides er digitalt signert. Nettleseren vil prøve å validere disse signaturene, og hvis den ikke får tak i adressene vil det ta lang tid å logge på (Java får en time out på nettkoblingen, og så kjøres appleten likevel). EPJ-systemet vil også ha behov for å validere signaturene som kommer fra kjernejournal mot Buypass sine tjenester.

Slik konfigurerer du sikker proxy:

1. Klikk på tannhjulet i nettleseren (innstillinger), og velg «Alternativer for Internett»
2. Velg fanen «Tilkoblinger» og klikk på knappen «LAN-innstillinger»

3. Velg «Avansert», og bildet under vil vises. Fyll ut som vist og klikk «OK»:



Sikker proxy er en mer begrenset åpning mot internett enn flex-proxy, men virksomheten må likevel vurdere om dette er en løsning de vil benytte seg av, gjennom sin risiko- og sårbarhetsanalyse.

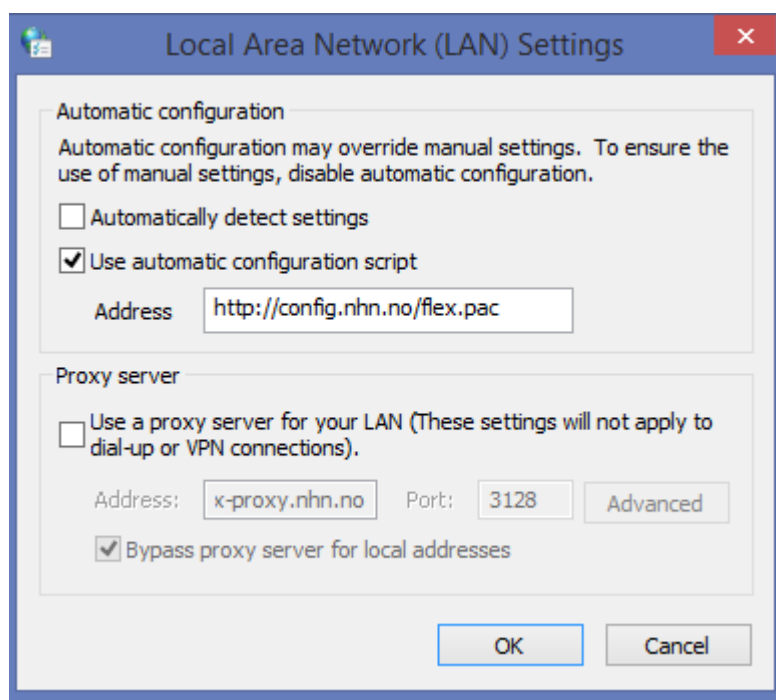
Se [Vedlegg 2](#)

Det er mulig å bruke NHN sin sikker-proxy. Denne benyttes bare til å få tak i helt spesifikke adresser (den er «white list»-basert) for antivirus-oppdateringer og sertifikatleverandører.

Det er mer informasjon tilgjengelig om denne tjenesten på NHN sine sider – se «Spørsmål og svar» her:

<https://www.nhn.no/hjelp-og-brukerstotte/helsenettet/Sider/default.aspx>

Hvis du bruker flex proxy, skal denne konfigureres slik:👇



Større driftsmiljøer (kommune, IKT-leverandører etc) må kanskje åpne manuelt for enkelte porter.

Komplett oversikt over nødvendige portåpninger finnes i [Vedlegg 3](#)

Tilkoblingssjekker (Buypass)

Tilgangen mot kjernejournal kan sjekkes manuelt ved at følgende sider kommer opp i en nettleser:

Forside	Link
Helsepersonellportalen	https://portal.kjernejournal.helsedirektoratet.no/hpp-webapp
Kjernejournal WS (viser tekst)	https://ws.kjernejournal.helsedirektoratet.no:8000/kjernejournal.sektor.kjernejournal/proxyservices/v1/Kjernejournal_HTTP?WSDL

Følgende adresser kan sjekkes i nettleser for Buypass.

Forside	Link
Buypass smartkortdiagnose	https://secure.buypass.no/wips/service?op=DIAG
Sjekk av revokeringstatus (laster ned)	http://ocsp.verisign.com

Forside	Link
fil)	
Sjekk av revokeringsstatus (laster ned fil)	http://sf.symcd.com

Hvis Java ikke har tilgang til Buypass applet vil Java bruke mye tid på å forsøke å nå disse adressene. Når den tilslutt feiler vil appleten allikevel lastes.

Hvis dette oppstår, se kapittel om: [Hvis lang påloggingstid](#)

Riktig klokke på PC og server

Kjernejournal helseindikator-tjeneste krever at klokka er synkronisert. Sikre at ditt miljø til enhver tid er synkronisert.

For å teste dette kan man benytte vår MiljøApp som tar en test av ditt oppsett. Se kapittelet [Hjelpemidler fra Direktoratet for E-helse - "Miljøapp"](#) for detaljer.

En mulig for å synkronisere miljøet på er å benytte Network Time Protocol (NTP) tjeneste. Erfaringsmessig trenger legekantorene ikke å bruke NHN sin NTP, så de som har NTP allerede kan benytte den de bruker.

Dersom miljøet ikke benytter NTP fra før kan NHN sin tjeneste ntp.nhn.no benyttes. For å sette opp NTP tjenesten på server og klient (anbefales å bli utført av en teknisk kyndig person):

<i>Hvis dere kjører domene og har flere domenekontrollere</i>	<i>Hvis dere bare har én domenekontroller</i>	<i>Hvis dere *ikke* bruker AD-domene</i>
Kjøre følgende kommando for å sjekke hvilken av dem som har rollen for å synkronisere klokke: netdom /query fsmo På serveren som blir rapportert, kjør følgende	På serveren som blir rapportert, kjør følgende kommandoer (bytt ut 0.0.0.0 med adressen til NHN-ruteren, som vil være default gateway eller ntp.nhn.no): w32tm /config	Kjøre følgende kommandoer på alle maskinene. Også pc' ene (bytt ut 0.0.0.0 med adressen til NHN-ruteren, som vil være default gateway eller ntp.nhn.no): w32tm /config

<i>Hvis dere kjører domene og har flere domenekontrollere</i>	<i>Hvis dere bare har én domenekontroller</i>	<i>Hvis dere *ikke* bruker AD-domene</i>
kommandoer (bytt ut 0.0.0.0 med adressen til NHN-ruteren, som vil være default gateway eller ntp.nhn.no): w32tm /config /manualpeerlist:"0.0.0.0,0x8" /syncfromflags:MANUAL /reliable:YES /update w32tm /resync /rediscover	/manualpeerlist:"0.0.0.0,0x8" /syncfromflags:MANUAL /reliable: YES /update w32tm /resync /rediscover	/manualpeerlist:"0.0.0.0,0x8" /syncfromflags:MANUAL /update w32tm /resync /rediscover

Oppdatering av operativsystemer på PC og servere

Enkelte servere eller klienter med gammelt operativsystem fra Microsoft, må ha service patches for at kjernejournalens web-service skal fungere.

Windows7

- KB977420 - A hotfix rollup is available to fix problems in Windows Communication Foundation in the .NET Framework 3.5 SP1 for Windows 7 and for Windows Server 2008 R2. [LINK](#).
(nedlasting: [LINK](#) . velg Windows6.1-KB977420-x86.msu)

Informasjon til brukerne

Alle brukere som skal benytte kjernejournal må sørge for at følgende steg er på plass:

- Brukeren må ha et personlig sertifikat, dvs. et smartkort utstedt av Buypass eller en USB-stick fra Commfides som er gyldig
- Brukeren må ha gyldig autorisasjon som helsepersonell i Norge, og dermed et HPR-nummer. Viktig at fullstendig personnummer (11 sifre) eller D-nummer er korrekt registrert i HPR register.
- Brukeren må ha godkjenningssprøve for kjernejournal for å benytte løsningen.

Sertifikater

Personlig sertifikat

Alle helsepersonell som skal logge seg inn på kjernejournal må ha PKI-sertifikat nivå 4 (utstedt av Buypass eller Commfides, med pin-kode - det samme som benyttes til e-resept, elektronisk sykemelding, etc.).

Bestilling av personlig sertifikat gjøres av EPJ-leverandøren, eller det kan gjøres her:

- Buypass: <http://www.buypass.no/Privat/Buypass+ID/Smartkort/Kortutstedere>
- Commfides: <https://e-id.commfides.com/>

Verifisere smartkort (Buypass)

Her kan du verifisere at personlig smartkort, IE og Java fungerer sammen.

1. Sett inn smartkort i kortleser
2. Trykk på følgende <https://secure.buypass.no/wips/service?op=DIAG>. (Trykk Yes/Continue på eventuell dialogboks som kommer opp)
3. Verifiser at kortinformasjon som vises er riktig
4. Trykk Fortsett
5. Bekreft at sertifikatinformasjon som vises er riktig
6. Trykk fortsett
7. Tast inn personlig kode i feltet «PIN kvalifiserte sertifikater» og trykk Bekreft
8. Du får et OK ved siden av feltet for PIN
9. Trykk X i høyre hjørne og du er ferdig med verifiseringen

Hvis du har problemer med disse stegene, ta kontakt med Buypass

Bruke eHelsebrukerportal for å sjekke personlig informasjon og ta godkjenningssprøve

NB! Brukeren må være tilkoblet Helsenettet

Kjernejournal har laget en eHelsebrukerportal der helsepersonell kan sjekke sin personlige kjernejournalinformasjon.

eHelsebrukerportal kan nåes via meny i EPJ eller på følgende adresse i Helsenettet: [LINK](#). Tilgang fås ved at brukeren er autentisert ved bruk av smartkort. Da vises disse opplysningene:

- Brukerens HPR informasjon, med lenke til HPR på [sak.no](#)
- Brukers tilganger i kjernejournal
- Link direkte til opplæring og oppslagsmateriell
- [LINK](#) til godkjenningssprøve dersom det ble funnet et HPR-nummer på personen
- [LINK](#) til driftstatus (informasjonsportalen)

Helsepersonell må gjennomføre opplæring og ha bestått en godkjenningssprøve for å få tilgang til kjernejournal. Fokus for prøven vil være det samme som for opplæringen: Hvilke opplysninger kjernejournal inneholder, hva den *ikke* inneholder, hvor opplysningene kommer fra og hvordan de skal brukes.

Status Helsepersonellregisteret

Denne informasjonen hentes fra HPR ved å bruke fødselsnummeret knyttet til smartkortet som ble benyttet i innloggingen. Dersom man ikke får noe informasjon fra HPR, kan det bety at man ikke har gyldig autorisasjon som helsepersonell eller at det er noe galt med koblingen HPR-fødselsnummer; i så tilfelle må man kontakte SAK for å få bistand til dette.

HPR-autorisasjon finnes	Feil i knytningen mellom HPR og fødselsnummer						
 <p>Helsepersonellregisteret</p> <p>For mer informasjon, se www.sak.no</p> <p>HPR-nummer: 222200063 (slå meg opp i www.sak.no)</p> <table><tr><td>Autorisasjon</td><td>Gyldig fra</td><td>Gyldig til</td></tr><tr><td>Lege</td><td>01.01.2010</td><td>01.01.2030</td></tr></table> <p>Kilde: Helsepersonellregisteret</p>	Autorisasjon	Gyldig fra	Gyldig til	Lege	01.01.2010	01.01.2030	 <p>Helsepersonellregisteret</p> <p>For mer informasjon, se www.sak.no</p> <p>Ingen autorisasjoner funnet på ditt fødselsnummer</p> <p>Kilde: Helsepersonellregisteret</p>
Autorisasjon	Gyldig fra	Gyldig til					
Lege	01.01.2010	01.01.2030					

Autorisasjon som helsepersonell

Alle som skal bruke kjernejournal som helsepersonell må ha en gyldig autorisasjon som helsepersonell i Norge. Dette administreres [helsedirektoratet](#). Det som er viktig i kjernejournalssammenheng er at HPR-nummeret er knyttet til fødselsnummeret på smartkortet. Dette har vist seg å være et problem på en del eldre brukere, og personer som har

hatt d-nummer tidligere. Denne tilknytningen kan verifiseres på [ebrukerportalen](#) som forklart over.

De fleste ligger korrekt registrert, men hvert enkelt helsepersonell bør kontrollere at informasjonen som er registrert på seg hos SAK faktisk er korrekt.

Dette er særlig aktuelt for leger under utdanning og leger som har fått norsk D-nummer/fødselsnummer etter at de fikk autorisasjon.

Det er viktig at det også finnes rutiner for håndtering av personlig sertifikat og kontroll av informasjonen i HPR-registeret for nye helsepersonell (vikarer, turnusleger og andre).

Slik kontrollerer du informasjonen i HPR-registeret:

1. Gå til [nettsidene til helsedirektoratet](#) og logg inn med personnummer
 - a. **NB!** Ikke logg på med HPR-nummer; det er informasjonen som er registrert på ditt fødselsnummer/ D-nummer du skal kontrollere
2. Resultatet blir vist på siden. Dersom informasjon om din autorisasjon ikke kommer frem eller ikke er korrekt, kan du selv oppdatere dette via Altinn.no

Det er viktig at fødselsnummer/ D-nummer i SAK er det samme som det som er knyttet til ditt personlige smartkort.

Kom i gang med kjernejournal

Kjernejournal er en brukervennlig og intuitiv løsning. Det er viktig at helsepersonell forstår hvordan de skal benytte kjernejournal. Derfor må de først gjennomføre opplæring.

Helsepersonell må ha bestått en godkjenningssprøve på for å få tilgang til kjernejournal. Fokus for prøven vil være det samme som for opplæringen: Hvilke opplysninger kjernejournal inneholder, hva den *ikke* inneholder, hvor opplysningene kommer fra og hvordan de skal brukes.

Lenke til nettbasert opplæring og godkjenningssprøven finner du her:

<https://ehelse.no/e-resept-kjernejournal-og-helsenorgeno/kjernejournal/godkjenningssprøve-og-opplering-i-kjernejournal>

Etter at kjernejournal er aktivert i EPJ og godkjenningssprøven er bestått, er det viktig å teste at funksjonaliteten fungerer.


NB!

Pass på at du kun åpner pasient med aktiv kjernejournal og som du har under behandling (dvs. har tjenstlig behov for å åpne) når du utfører denne testen.

Alternativt kan du åpne kjernejournal på deg selv.

Testen er som følger:

1. Åpne en pasient i EPJ systemet og se at helseindikator-knapp vises

Helseindikator	Symboliserer
	Pasienten har kjernejournal
	Pasienten har kjernejournal med registreringer i pasientens felter
	Pasienten har kjernejournal med kritisk informasjon

2. Trykk på helseindikator-knapp og velg Buypass- eller Commfidespålogging for å logge inn
3. Kjernejournalportalen åpnes for valgte pasient

Dersom alle punktene over er gjennomført OK er dere ferdig med forberedelsene og kjernejournal er aktivert.

Hvis du har problemer med disse stegene, ta kontakt med EPJ-leverandør.

3 Vedlegg

Vedlegg 1: Problemløsning

Hvis lang påloggingstid (Buypass)

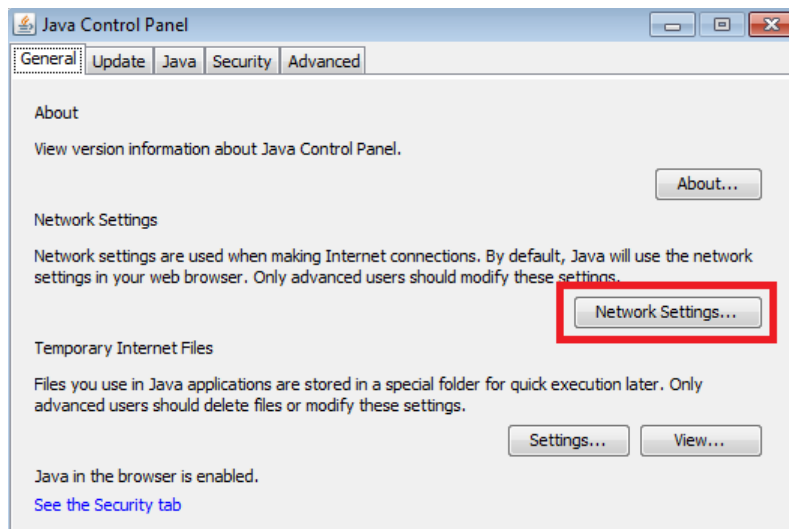
Hvis pålogging til Buypass tar lang tid selv etter den har blitt lastet ned første gang skyldes dette sjekker til nettverksadresser som feiler. Appleten vil etter en viss tid forsete og laste opp som normalt. Hvis følgende bilde under vises i mer enn 10 sekunder er det sannsynlig at problemet er til stede. Se **Sjekk Java Proxy Innstillinger** og **Oppgrader Java** under for å løse problemet.

2. Figure 1 Bypass applet laster

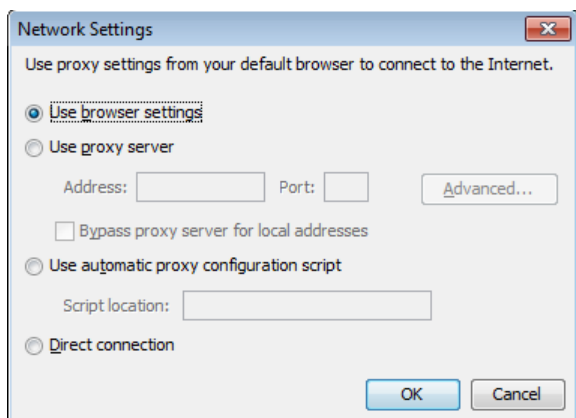


Sjekk Java Proxy Innstillinger

1. Start Windows **Start-meny** eller **Start-skjerm**
2. Klikk **Alle Programmer** (hvis den vises)
3. Finn **Java** og klikk på Java for å få listet opp underelementene
4. Klikk **Konfigurer Java / Configure Java** snarvei for å starte Java Control Panel
5. Klikk **Nettverk Innstillinger / Network Settings...**



Hvis annet valg enn **Oppdag innstillinger automatisk / Use browser settings** vil dette overstyre innstillingene som gjelder for nettleser. Det kan bety at Java benytter feil strategi for å nå <http://ocsp.verisign.com> og <http://sf.symcd.com>. Sett valget til **Oppdag innstillinger automatisk / Use browser settings**. Hvis legekantoret har **Automatisk konfigurering / Use automatic proxy configuration script**, ta kontakt.



Oppgrader Java

Hvis **Oppdag innstillinger automatisk / Use browser settings** er satt og det ikke fikser problemet kan årsaken være gammel Java-versjon. Det har vist seg at noen gamle Java-versjoner ikke leser proxy-innstillingene fra nettleser som er nødvendig for å nå Helsenettet. Da må Java-versjonen oppgraderes. Kjernejournal anbefaler å oppgradere til siste versjon av Java 8. Se kapittelet om å oppgradere Java lenger opp i dokumentet.

Vedlegg 2: Risiko- og sårbarhetsanalyse

Hver enkelt virksomhet er ansvarlig for å gjennomføre Risikovurderinger av sin behandling av helse- og personopplysninger. En innledning til dette teamet er beskrevet i Norm for informasjonssikkerhet for Helse- og omsorgstjenesten.

<https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet>

Som databehandlingsansvarlig for kjernejournal har Helsedirektoratet gjennomført flere Risiko og Sårbarhetsanalyser (RoS), som en integrert del av etableringsprosessen. For å understøtte virksomhetene som skal bole seg opp til kjernejournal med sine RoS-analyser, legger vi ved noen relevante betraktninger og innspill.

Bruk av NHN sin GT-Sikker Proxy-tjeneste

Denne tjenesten åpner for trafikk fra helsenettet ut mot noen få, utvalgte internettsadresser. Det er åpnet mot antivirus-oppdateringstjenester, sertifikat-tjenester samt noe programvareoppdateringer.

NHN har en egen RoS-analyse for denne tjenesten, tilgjengelig på helsenettet:

<https://nhn.no/hjelp-og-brukerstotte/helsenettet/Sider/risikovurderinger.aspx>

Tabellen nedenfor lister opp noen relevante trusler som virksomheten bør vurdere, samt noen innspill til hvordan truslene kan vurderes:

Hendelse/Trussel	Tiltak	Sannsynlighet	Konsekvens
EPJ sender sensitive personopplysninger ut på internett	Eksisterende: <ul style="list-style-type: none"> • EPJ skal ikke gjøre dette, uavhengig om den har internettkobling eller ikke • Det er bare noen spesifiserte URL'er det er åpnet for, og dette er med å begrense konsekvensen 	Denne er i den lave enden av skalaen, da dette forutsetter grov feil eller misbruk av EPJ	Denne er i den høye enden av skalaen. Den er kanskje ikke på høyeste nivå, ettersom det er et fåtall URL'er man faktisk kan lekke sensitive opplysninger til.
Andre systemer enn EPJ sender sensitive personopplysninger ut på internett	Eksisterende: <ul style="list-style-type: none"> • Det er bare noen spesifiserte URL'er det er åpnet for, og dette er med å begrense 	Denne er i den lavere til midtre enden av skalaen, uten ekstra tiltak hos virksomheten.	Denne er i den høye enden av skalaen. Den er kanskje ikke på høyeste nivå, ettersom det er et fåtall URL'er man

Hendelse/Trussel	Tiltak	Sannsynlighet	Konsekvens
	konsekvensen Virksomhet bør vurdere <ul style="list-style-type: none"> Sørge for at det kun er systemer/servere med et konkret behov som faktisk kan bruke denne proxyen Gjennomgang av sine rutiner for hvor og hvordan personopplysninger behandles. 		faktisk kan lekke sensitive opplysninger til.
En angriper får tilgang til virksomhetsinterne systemer gjennom proxy	Eksisterende <ul style="list-style-type: none"> Tjenesten er bygget for å motvirke akkurat denne typen angrep. Referer til NHN sin dokumentasjon og RoS for ytterlige detaljer 	Denne ligger i den lave enden av skalaen, gitt NHN sine tiltak rundt tjenesten.	Denne vil trolig ligge med høyeste konsekvens, litt avhengig av virksomhetens tiltak

Bruk av NHN sin tjeneste Flex proxy

Denne tjenesten åpner for trafikk fra helsenettet ut mot store deler av internett. Det er en liste over adresser som ikke er tilgjengelig (black list). Denne kan blant annet benyttes til å få tak i Commfides sin applet for innlogging.

NHN har en egen RoS-analyse for denne tjenesten, tilgjengelig på helsenettet:

<https://nhn.no/hjelp-og-brukerstotte/helsenettet/Sider/risikovurderinger.aspx>

For å bruke kjernejournal på en sikker måte er det anbefalt å benytte kombinasjonen av GT-Sikker Proxy og endring av host DNS (beskrevet nedenfor), men for noen kan det hende Flex proxy allerede er i bruk, eller passer bedre.

Tabellen nedenfor lister opp noen relevante trusler som virksomheten bør vurdere, samt noen innspill til hvordan truslene kan vurderes:

Hendelse/Trussel	Tiltak	Sannsynlighet	Konsekvens
------------------	--------	---------------	------------

Hendelse/Trussel	Tiltak	Sannsynlighet	Konsekvens
EPJ sender sensitive personopplysninger ut på internett	Eksisterende: <ul style="list-style-type: none"> EPJ skal ikke gjøre dette, uavhengig om den har internettkobling eller ikke 	Denne er i den lave enden av skalaen, da dette forutsetter grov i feil eller misbruk av EPJ	Denne vil trolig ligge med høyeste konsekvens, litt avhengig av virksomhetens tiltak
Andre systemer enn EPJ sender sensitive personopplysninger ut på internett	Virksomhet bør vurdere <ul style="list-style-type: none"> Sørge for at det kun er systemer/servere med et konkret behov som faktisk kan bruke denne proxyen Gjennomgang av sine rutiner for hvor og hvordan personopplysninger behandles. 	Denne er i den lavere til midtre enden av skalaen, uten ekstra tiltak hos virksomheten.	Denne vil trolig ligge med høyeste konsekvens, litt avhengig av virksomhetens tiltak
En angriper får tilgang til virksomhetsinterne systemer gjennom proxy	Eksisterende <ul style="list-style-type: none"> Tjenesten er bygget for å motvirke akkurat denne typen angrep. Referer til NHN sin dokumentasjon og RoS for ytterlige detaljer 	Denne ligger i den lave enden av skalaen, gitt NHN sine tiltak rundt tjenesten.	Denne vil trolig ligge med høyeste konsekvens, litt avhengig av virksomhetens tiltak

Slå av signering av Java applets

Det kan være verdt å vurdere å slå av Java sin signaturvalidering på Java-applets. Dermed vil ikke Java prøve å validere signaturen før innlogging, og man har ikke behov for å bruke noen proxy for dette formålet. (Det er mulig man trenger proxy for andre formål, men det må vurderes separat.)

Tabellen nedenfor lister opp noen relevante trusler som virksomheten bør vurdere, samt noen innspill til hvordan truslene kan vurderes:

Hendelse/Trussel	Tiltak	Sannsynlighet	Konsekvens
Nettleser laster ned en falsk applet fra en usikker URL, og kjører denne	<p>Eksisterende</p> <ul style="list-style-type: none"> Kjernejournal peker på en https-adresse for nedlasting av applet, med gyldige TLS-sertifikater <p>Virksomhet bør i det minste</p> <ul style="list-style-type: none"> Validere TLS-kanalen, sånn at denne er trygg 	Gitt begge tiltak er ligger denne i laveste ende av skalaen	Denne vil trolig ligge med høyeste konsekvens
Nettleser laster ned en falsk applet fra korrekt URL, og kjører denne	<p>Eksisterende</p> <ul style="list-style-type: none"> Buypass er en partner vi har tillit til, og de har rutiner for å hindre dette. For dem er tillit virksomhetskritisk 	Denne kan trolig plasseres i laveste ende av skalaen	Denne vil trolig ligge med høyeste konsekvens

Endre DNS- eller host-oppsett for Buypass-adresser

Formål	Formålet med dette er å gjøre seg helt uavhengig av internettkoblinger
Hvordan det virker	<p>Sertifikatene til Buypass inneholder adresser for validering som ligger på internett, og man kan bruke proxy for å få tak i denne (GT-Sikker proxy eller Flex Proxy).</p> <p>Dette alternativet, med å endre DNS eller host-fil, går ut på å sørge for at EPJ-systemer som etterspør disse adressene havner på en egen Buypass-node i helsenettet.</p>
Hva må til	<p>For de fleste systemer er det mest aktuelt å endre host-filen i Windows:</p> <p>91.186.95.65 ojsp.buypass.no 91.186.95.66 crl.buypass.no 91.186.95.64 ldap.buypass.no</p>
Alternativt	For større datasentre kan det være aktuelt å gjøre slike grep i

	intern DNS
Risikobetraktning	Disse endringene er i hovedsak en tilgjengelighetstrussel for EPJ, da det kompliserer oppsettet i legekontoret noe. Dette må virksomheten vurdere opp mot gevinsten av å slippe å bruke proxy mot internett

Vedlegg 3: Oversikt over nødvendige portåpninger for Kjernejournal

Kjernejournal

Selve kjernejournal har to IP-adresser, én for portalen og én for webservicen. I tillegg benyttes Commfides eller Bypass til innlogging.

Beskrivelse	IP-adresse	Port	Nett	DNS-navn
Kjernejournal portal	91.186.92.85	443	Helsenett	portal.kjernejournal.helsedirektoratet.no
Kjernejournal WS	91.186.92.86	8000	Helsenett	ws.kjernejournal.helsedirektoratet.no
Bypass innloggingsside	91.186.95.67	443	Helsenett	secure.nhn.bypass.no
Commfides innloggingsside	91.186.95.27	443	Helsenett	app05.commfides.com

Revokeringssjekk

I tillegg vil det normalt sett være nødvendig å nå Bypass sine revokeringstjenester, for revokeringssjekk av kjernejournalens sertifikater. Disse tjenestene er publisert både på helsenettet og internett – bruker man Norsk Helsenett sin DNS-tjeneste, vil man bli pekt mot helsenett-adressene, ellers vil de peke mot internett-adressene.

Beskrivelse	IP-adresse	Port	Nett	DNS-navn			
Revokeringssjekk av TLS- og Virksomhetssertifikater INTERNETT	185.62.160.144	80	Internett	ocsp.bypass.no			
	185.62.162.144						
	185.62.160.145	80	Internett	crl.bypass.no			
	185.62.162.145						
	185.62.160.146				389	Internett	ldap.bypass.no
	185.62.162.146						
Revokeringssjekk av TLS- og Virksomhetssertifikater HELSENETT	91.186.95.64	389	Helsenett	ldap.bypass.no			
	91.186.95.65	80	Helsenett	ocsp.bypass.no			
	91.186.95.66	80	Helsenett	crl.bypass.no			

NB: Legg merke til at Bypass har to ip-adresser per tjeneste på internett.

Java krever ekstra adresser

Hvis man benytter seg av Java for innlogging (dvs. Commfides eller Buypass sin Java-løsning), er Java avhengig av noen ekstra adresser. De er kun tilgjengelig på internett:

Beskrivelse	IP-adresse	Port	Nett	DNS-navn
Kun for Commfides Java-applet	178.255.83.1	80	Internett	ocsp.usertrust.com
Kun for Commfides Java-applet	178.255.83.1	80	Internett	ocsp.comodoca.com
Kun for Commfides Java-applet	93.184.220.20	80	Internett	cdp1.public-trust.com
Kun for Commfides Java-applet	62.48.217.196	80	Internett	ocsp.multicert.com
Kun for Commfides Java-applet	156.151.59.19	80	Internett	java.sun.com
Kun for Commfides Java-applet	**	80	Internett	www.oracle.com
Kun for Buypass Java-applet	**	80	Internett	ocsp.verisign.com
Kun for Buypass Java-applet	**	80	Internett	sf.symcd.com

** Legge merke til at ocsp.verisign.com, sf.symcd.com og www.oracle.com kjører i Akamai sin CDN-løsning, slik at de ikke har noen fast ip-adresse. Derfor er man i praksis avhengig av en proxy for å kunne åpne opp for disse.

Disse åpningene slipper man da unna om man benytter seg av Buypass sin javafrie løsning.

Oversikt over URL'er for Kjernejournal

URL-en til kjernejournal sin webservice (HentHelseindikasjon) er som følger:

https://ws.kjernejournal.helsedirektoratet.no:8000/kjernejournal.sektor.kjernejournal/proxyserVICES/v1/Kjernejournal_HTTP

URL-ene til kjernejournal-portalen varierer etter hvilken innloggingsmetode man benytter seg av:

Buypass Java-innlogging:


Beskrivelse	URL
Helsepersonellportalen	https://portal.kjernejournal.helsedirektoratet.no/hpp-webapp
Godkjenningssprøven for helsepersonell	https://portal.kjernejournal.helsedirektoratet.no/gkp-webapp?prove=HELSEPERSONELL
eHelsebrukerportalen	https://portal.kjernejournal.helsedirektoratet.no/ebp-webapp

Buypass Javafri-innlogging:

Beskrivelse	URL
Helsepersonellportalen	https://portal.kjernejournal.helsedirektoratet.no/hpp-webapp/buypassjavafri
Godkjenningssprøven for helsepersonell	https://portal.kjernejournal.helsedirektoratet.no/gkp-webapp/buypassjavafri?prove=HELSEPERSONELL
eHelsebrukerportalen	https://portal.kjernejournal.helsedirektoratet.no/ebp-webapp/buypassjavafri

Commfides-innlogging:

Beskrivelse	URL
Helsepersonellportalen	https://portal.kjernejournal.helsedirektoratet.no/hpp-webapp/commfides
Godkjenningssprøven for helsepersonell	https://portal.kjernejournal.helsedirektoratet.no/gkp-webapp/commfides?prove=HELSEPERSONELL
eHelsebrukerportalen	https://portal.kjernejournal.helsedirektoratet.no/ebp-webapp/commfides

 Direktoratet for e-helse

Besøksadresse

Verkstedveien 1
0277 Oslo

Postadresse

Postboks 6737
St. Olavs plass
0130 OSLO