

**Brukerdokumentasjon av krypteringsprogrammet RegKrypt**

**Versjon 1.1**

**24.03.2014/TJ,MG**

**Helsedirektoratet**

**Endringshistorikk**

|  |  |  |
| --- | --- | --- |
| **Versjonsnr** | **Dato** | **Beskrivelse av endringer** |
| 1.0 |  |  |
| 1.1 | 24.03.2014 | Kun endring av link-adresser |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Innhold**

[1. Innledning 4](#_Toc346531765)

[1.1 Om dokumentet 4](#_Toc346531766)

[1.2 Målgruppe 4](#_Toc346531767)

[1.3 Sikkerhet 4](#_Toc346531768)

[2. Oversikt over registersammenstilling 5](#_Toc346531769)

[3. Installering av RegKrypt 6](#_Toc346531770)

[3.1 Forutsetninger 6](#_Toc346531771)

[3.2 RegKrypt 6](#_Toc346531772)

[3.2.1 Konfigurasjon 6](#_Toc346531773)

[3.3 Krypteringsnøkler 6](#_Toc346531774)

[3.4 RegBestilling 7](#_Toc346531775)

[4. Bruk av RegKrypt 8](#_Toc346531776)

[5. Bruk av RegBestilling 10](#_Toc346531777)

# Innledning

Krypteringsprogrammet RegKrypt er en tilpasset versjon av programmet Veiviseren som er utviklet av Folkehelseinstituttet. Veiviseren benyttes av forskere i forbindelse med sammenstilling av registerdata med Reseptregisteret. RegKrypt skal benyttes i forbindelse med sammenstilling av registerdata med IPLOS registeret.

RegKrypt krypterer en kommaseparert fil med registerdata og genererer en xml fil som sendes til IPLOS registeret for å sammenstille registerdata med IPLOS data.

## Om dokumentet

Dette dokumentet beskriver installasjon og bruk av krypteringsprogrammet RegKrypt.

Siste versjon av dokumentet kan hentes fra:

<http://www.ssb.no/innrapportering/offentlig-sektor/iplos>

## Målgruppe

Målgruppen for dokumentet er forskere som skal sammestille registerdata med data fra IPLOS registeret. Det kreves en viss kjennskap til informasjonsteknologi (IT) for å lese deler av dette dokumentet.

## Sikkerhet

Registerdata som sendes fra forskerne til IPLOS registeret skal krypteres av RegKrypt. De krypterte data blir sendt til Tiltrodd PseudonymForvalter (TPF), som er den instans som erstatter fødselsnummer med pseudonymer på vegne av databehandlingsansvarlig for registeret som er Helsedirektoratet. Helseregisterloven krever at TPF skal være uavhengig av databehandler og av den databehandlingsansvarlige. Skattedirektoratet er TPF for IPLOS-registeret.

De krypterte og pseudonymiserte registerdata sendes videre til IPLOS registeret hos SSB.

# Oversikt over registersammenstilling

Registersammenstilling utføres av flere programmoduler.



Prosessen for å gjennomføre en registersammenstilling starter med at en forsker har en datamengde som betegnes som registerdata. Denne datamengden kan komme fra helseregistre, helseundersøkelser, forskerens egne data og lignende. Registerdata inneholder for hver person et fødselsnummer og en liste med persondata.

Forskeren kjører RegKrypt på en PC i en sikker sone. Sonen har ikke tilgang til Internett. Inndata til RegKrypt er registerdata som er en kommaseparert fil. RegKrypt vil kryptere persondata med en offentlig krypteringsnøkkel for IPLOS registeret, og så kryptere resten av meldingen unntatt meldingstype og avsender med en offentlig krypteringsnøkkel for TPF.

Den krypterte meldingen overføres manuelt til en PC i åpen sone som har tilgang til Internett. Her aksesserer man RegBestilling som har en webadresse hos Tiltrodd PseudonymForvalter. RegBestilling leser den krypterte meldingen og sender den til TPF systemet. Hos TPF blir den delen av meldingen som inneholder fødselsnummer dekryptert og fødselsnummer skiftet ut med pseudonym. Deretter sendes meldingen videre til IPLOS registeret hos SSB. TPF har ikke mulighet for å dekryptere resten av meldingen som inneholder persondata.

Hos SSB vil saksbehandlere sammenstille de mottatte persondata med data fra IPLOS registeret, og sende de sammenstilte data til forskeren såfremt data er på anonym form.

# Installering av RegKrypt

## Forutsetninger

##### Kompetanse

Det kreves en viss kjennskap til informasjonsteknologi for å installere programvare og sende registerdata. Det forutsettes at denne operasjonen foretas av en IT-kyndig forsker.

##### Operativsystem

RegKrypt kan brukes under følgende operativsystem:

* Microsoft Windows XP/Vista/7 eller nyere, både 32- og 64 bit versjoner.

##### Nettleser

Nettleser bør være oppdatert til dagens versjon.

## RegKrypt

RegKrypt krever at .Net Framework minimum versjon 3.5 finnes på PC-en i sikker sone. Dersom den ikke finnes kan den lastes ned sammen med krypteringsmodulen. Det er derfor to filer for nedlastning:

1. dotnetfx35.exe (231 MB). Inneholder .NET Framework versjon 3.5, som er nødvendig for å kjøre .NET-baserte applikasjoner. Merk at det ikke er nødvendig å bry seg om denne filen dersom man vet at denne eller nyere rammeverksversjon allerede er installert.
2. RegKryptSetup.msi (3 MB). Pakken inneholder RegKrypt programmet.

Siste versjon av en installasjonspakke kan lastes ned fra:

<http://www.ssb.no/innrapportering/offentlig-sektor/iplos>

Når filene er nedlastet overføres de til en PC i sikker sone. Eventuelt kan gammelt RegKrypt fjernes med Add/Remove programs. Installasjonen igangsettes ved å først dobbeltklikke på dotnetfx35.exe, dersom rammeverksversjonen ikke allerede er installert. Deretter dobbeltklikkes RegKryptSetup.msi.

### Konfigurasjon

Etter installasjon av RegKrypt vil det på installasjonskatalogen ligge en fil med navn RegKrypt.exe.config.Eksempel

Kopier denne, og gi kopien navn RegKrypt.exe.config

Det er ikke nødvendig å endre denne konfigurasjonsfila.

## Krypteringsnøkler

Siste versjon av offentlig krypteringsnøkkel for TPF og for IPLOS registeret kan lastes ned fra:

<http://www.ssb.no/innrapportering/offentlig-sektor/iplos>

Det blir lagt ut nye versjoner den 1. desember hvert år. Når krypteringsnøkkelfilen er nedlastet må den overføres til en PC i sikker sone. Filen med krypteringsnøkler lagres som filtype .xml eller .txt, og encoding = Unicode.

## RegBestilling

Sendemodulen anvendes via Internett, og skal ikke installeres.

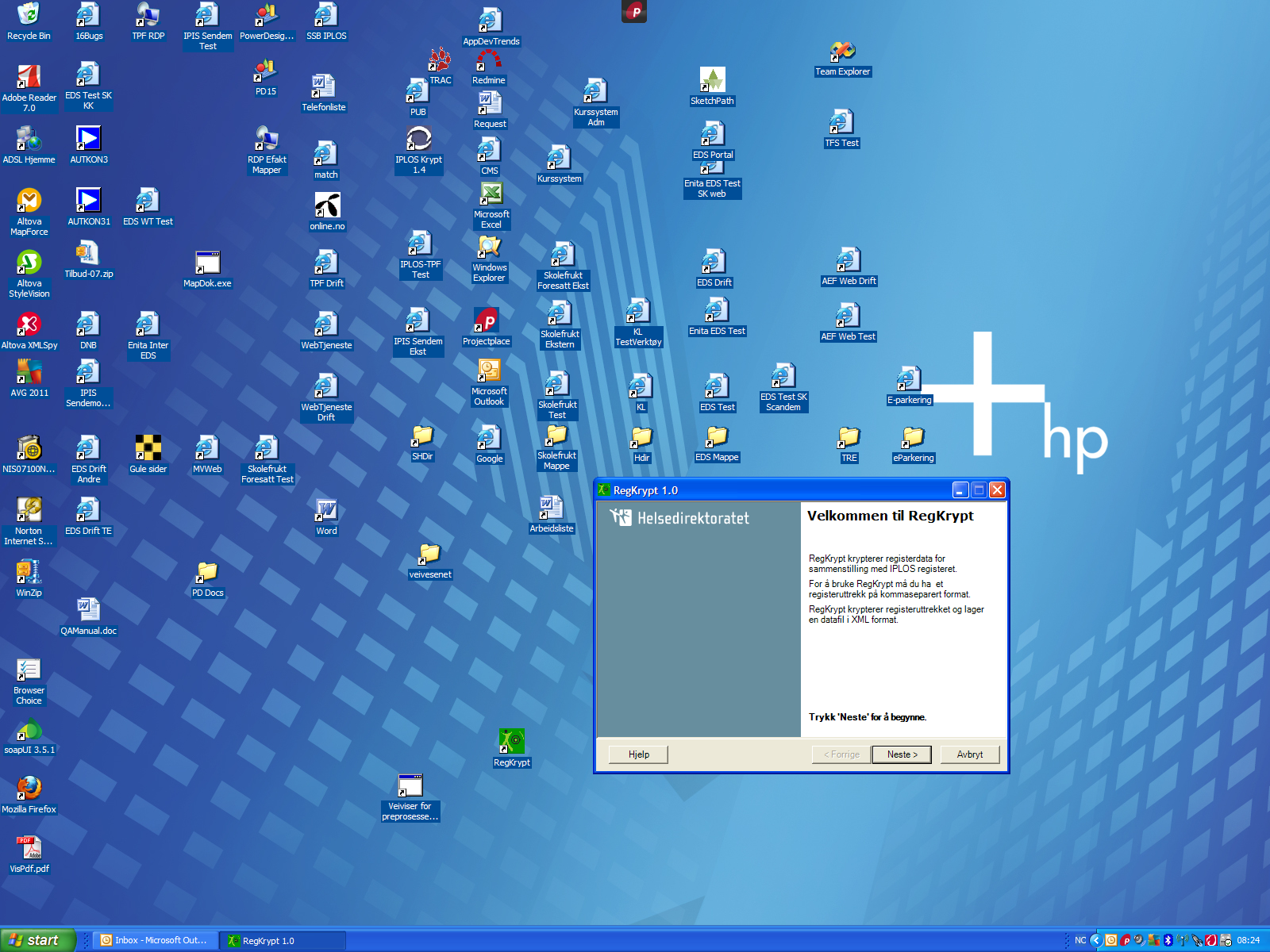
# Bruk av RegKrypt

##### Hensikt

Programmet benyttes til å lese en fil med registerdata og kryptere filen. Det benyttes offentlig krypteringsnøkkel fra IPLOS registeret og fra TPF.

**Beskrivelse**

Brukeren starter programmet RegKrypt som ligger i startmenyen og skjermbildet nedenfor vises.



Eksempel på skjermbilde

Brukeren klikker seg gjennom flere skjermbilder og gjør følgende:

1. Registrer avsendernavn, prosjektnummer, registernavn og løpenummernøkkel.   
   OBS: Prosjektnummer må være eksakt lik saksnummeret som er mottatt fra Helsedirektoratet.
2. Velg skilletegn; komma eller semikolon. Velg registerdatafil som skal krypteres. *Registerdatafil må være lagret med tegnsett utf-8* (med tegnsett ANSI/ISO-8859 vil norske tegn bli feil).
3. Velg fil med krypteringsnøkler  
   RegKrypt genererer:
   1. kryptert xml fil som lagres med samme filnavn som registerdatafilen, men med ”.xml” endelse.
   2. Fil som bare er kryptert med IPLOS krypteringsnøkkel. Lagres med samme navn som registerdatafilen, men med ”-HosKilde.xml” endelse.
   3. Hvis disse to xml filene allerede eksisterer vil de bli overskrevet.

RegKrypt er ferdig og skriver sammendrag.

Brukeren kan så overføre den krypterte filen til en PC i åpen sone og fortsette med RegBestilling, se neste kapittel.

**Feilmeldinger**

Følgende feilmeldinger vil medføre at kjøringen avsluttes og det blir ikke generert noen kryptert fil:

* **Registerdatafilen kunne ikke åpnes.**

# Bruk av RegBestilling

##### Hensikt

Programmet benyttes til å lese en fil med krypterte registerdata og sende filen til TPF.

Brukere av RegBestilling vil være forskere og saksbehandlere i Helsedirektoratet.

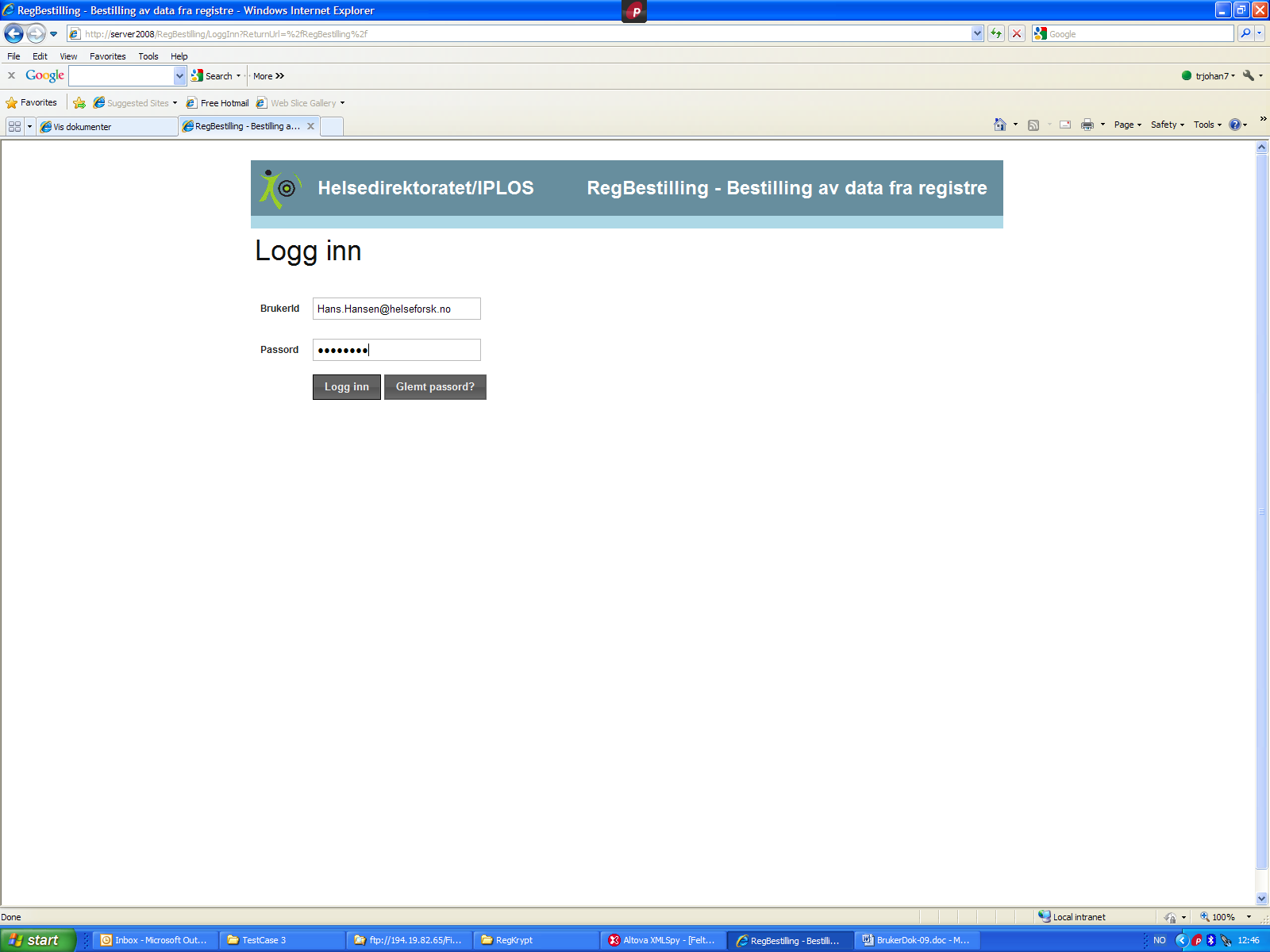
**Beskrivelse**

Når prosjektet er blitt godkjent i Helsedirektoratet, vil leder for forskningsprosjektet få tilsendt brukerid og passord til RegBestilling.

Forskeren starter programmet ved å klikke på:

<https://iplos.skatteetaten.no/regbestilling/>

Skjermbildet for innlogging vil vises.

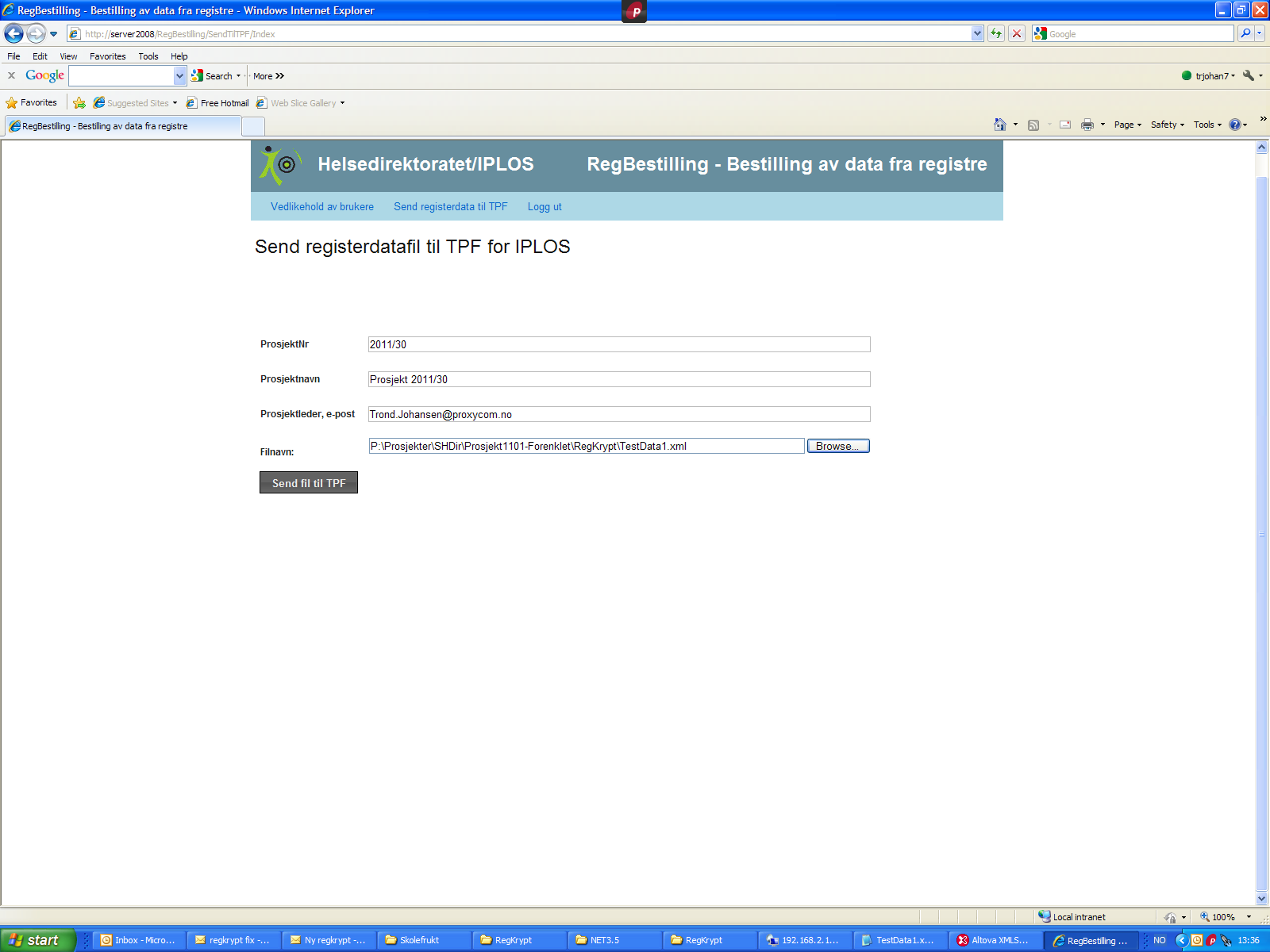


Eksempel på skjermbilde for innlogging

Forskeren registrerer: BrukerId, passord og klikker ”Logg inn”.

Forskere som har glemt passord kan klikke på knappen: ”Glemt passord” og få tilsendt passord via e-post.

Blir de registrerte verdier godtatt så vil programmet vise en meny. Forskeren kan klikke på: ”Send registerdata til TPF” og systemet skriver prosjektnr, prosjektnavn og e-postadressen til prosjektleder.



Eksempel på skjermbilde for sending.

Forskeren klikker på ”Browse”, finner den krypterte registerdatafilen og klikker på ”Send fil til TPF”. Systemet vil utføre følgende:

* Vise teksten: ”Sendingen startet kl 10:12
* Lese filen
* Sende filen videre til TPF
* Programmet avslutter med å skrive kvitteringen: ”Sending ferdig kl 10:14”.

Det anbefales at brukeren tar en utskrift av skjermbildet som kvittering når sending er utført.

I tillegg er det et annet valg i menyen der forskeren kan endre passord og opprette nye brukere som skal ha adgang til prosjektet i RegBestilling.

**Feilmeldinger**

Følgende feilmeldinger vil medføre at kjøringen avsluttes og kryptert registerdata fil blir ikke sendt:

* **Ugyldig format på kryptert melding. Kjøringen avsluttes**
* **Feil ved sending av fil; Ikke gyldig XML.**
* **Valideringsfeil. Ukjent tag navn: ........**

Kontroller at den spesifiserte krypterte registerdata fil virkelig er en fil som er generert av RegKrypt.

Dersom filen likevel ser ut til å være riktig tas kontakt med *IPLOS ansvarlig hos SSB*.