

Hva er SAFE?

Kort introduksjon

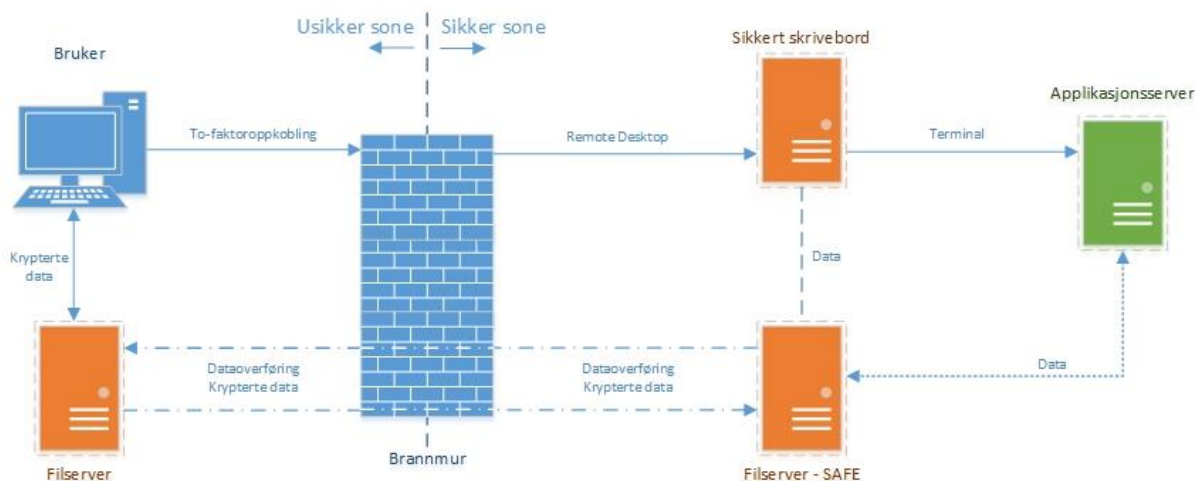
På IT-avdelingen ved Universitetet i Bergen har vi utviklet en løsning for sikker behandling av sensitive personopplysninger i forskning. Løsningen kaller vi SAFE (Sikker Adgang til Forskningsdata og E-infrastruktur). SAFE bygger på Norm for informasjonssikkerhet i helse- og omsorgstjenestene (Normen) og sikrer at informasjonssikkerheten med hensyn til konfidensialitet, integritet og tilgjengelighet blir ivaretatt ved behandling av sensitive personopplysninger.

Gjennom SAFE tilbyr IT-avdelingen en løsning der ansatte, studenter og eksterne får tilgang til dedikerte ressurser for behandling av sensitive personopplysninger.

Som leder for eller deltager i et forskningsprosjekt får du tilgang til et sikkert skrivebord i SAFE. Regnekraft og relevant programvare er tilgjengelig fra det sikre skrivebordet. Prosjektleder styrer tilgang til prosjektet og har oversikt over hvilke data som overføres ut fra SAFE.

Prinsippskisse

I SAFE opererer vi med en sikker sone, SAFE, og en usikker-sone, som i praksis er resten. Dette betyr selvfølgelig ikke at data ikke kan sikres andre steder enn i SAFE. Prinsippet er illustrert i følgende figur:



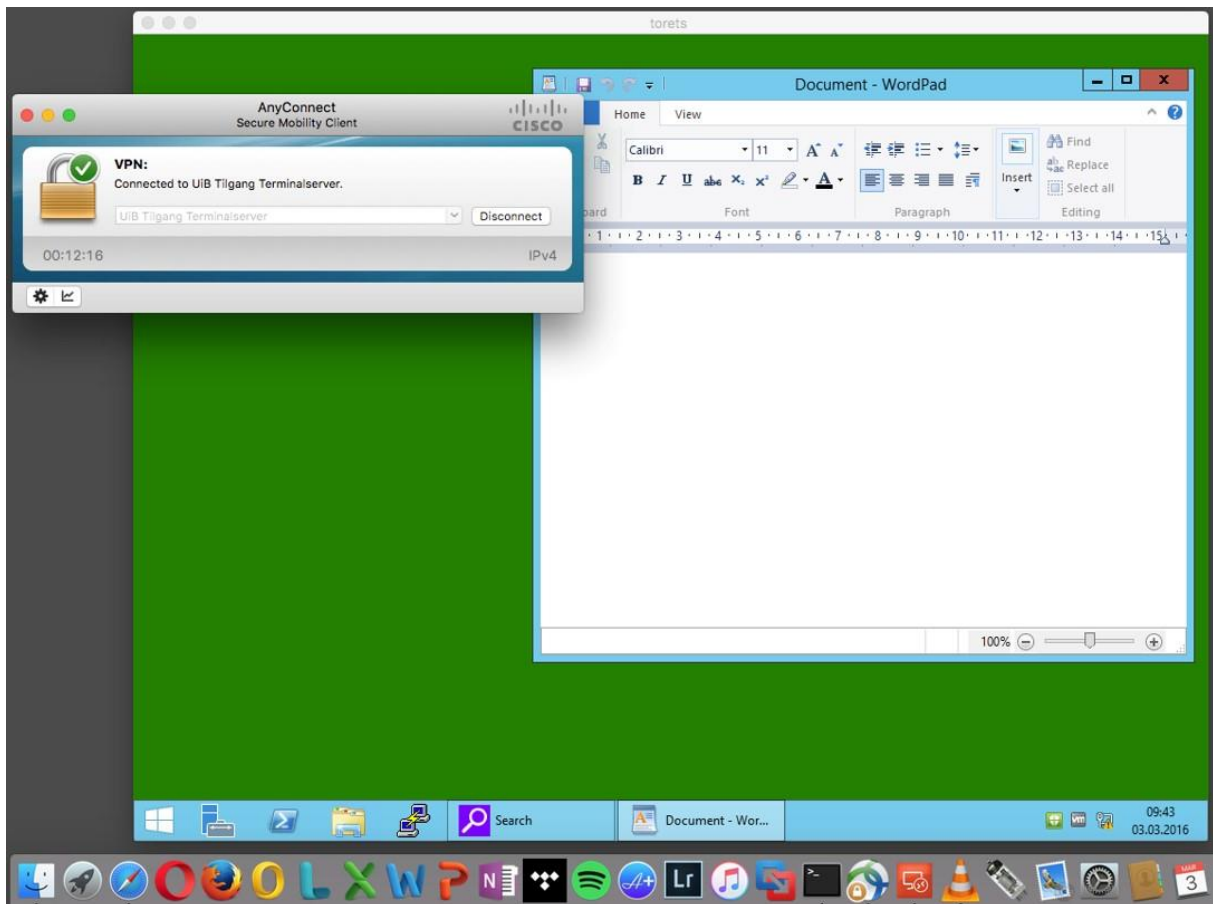
Slik løsningen er satt opp, kobler du deg mot SAFE fra din egen datamaskin ved å bruke en VPN-klient som støtter 2-faktor. VPN klienten sørger for at du kommer på innsiden av brannmuren, i den sikre sonen som vi kaller SAFE. Herfra kobler du deg til det sikre skrivebordet. Fra det sikre skrivebordet kan du starte programmer og nå data i prosjektet. De som har behov kan også koble seg opp mot en dedikert Linux applikasjonsserver fra det sikre skrivebordet.

Filer kan flyttes til og fra SAFE fra din egen klient ved import og eksport. Vi kommer tilbake til hvordan import og eksport virker etterhvert.

Hvilken programvare du skal bruke for å koble deg mot SAFE og det sikre skrivebordet avhenger av hvilket operativsystem du bruker. Vi kommer tilbake til hvordan du installerer og bruker programmene for ditt operativsystem etterhvert.

Sikkert skrivebord

Bildet under viser hvordan et sikkert skrivebord kan se ut. I bakgrunnen i dette eksempelet vises et typisk Mac-skrivebord og i forgrunnen vises VPN-klienten som ble brukt for å koble til SAFE. Den grønne arbeidsflaten er det såkalte sikre skrivebordet.



Sikring av skrivebordet

Sikring av skrivebordet er todelt.

1. Tilgang til sikkert skrivebord krever to-faktor autentisering. Både noe du vet (brukernavn og passord) og noe du har (engangskode som tekstmelding eller i app på smarttelefon).
2. Begrensede muligheter fra det sikre skrivebordet. Du kan ikke:
 - koble deg mot nettsider på utsiden av SAFE
 - overføre filer til eller fra dataområder på utsiden av SAFE (mulig gjennom slusen)
 - skrive ut dokumenter fra SAFE

Hvis du er interessert, kan du videre lese hva Datatilsynet sier om når det er krav til sterkere autentisering.

"Når er det krav om sterkere autentisering (for eksempel to-faktor) enn bare brukernavn og passord?"

Vi stiller krav til sterk autentisering når en person har tilgang til et informasjonssystem med sensitive personopplysninger og/eller personopplysninger om mange over eksterne nett. Dersom uvedkommende klarer å skaffe seg et brukernavn og passord, vil det uten flere hindre være mulig å logge seg på informasjonssystemet fra hvor som helst. Det kan de gjøre når som helst.

Brukernavn er ofte statisk og lett å gjette seg til. Passord er også mulig å finne ut av. Uten et tiltak i tillegg til brukernavn og passord, er opplysningene ikke godt nok sikret. Sterk autentisering gjør det vanskeligere for noen som får tak i brukernavn og passord å skaffe seg tilgang til systemet.

Med sterk autentisering mener vi for eksempel bruk av kodebrikke eller sikkerhetskode tilsendt på SMS, i tillegg til brukernavn og passord. Dette kan også realiseres i en fjernarbeidsløsning med sterk autentisering, og påfølgende tilgang til informasjonssystemet."