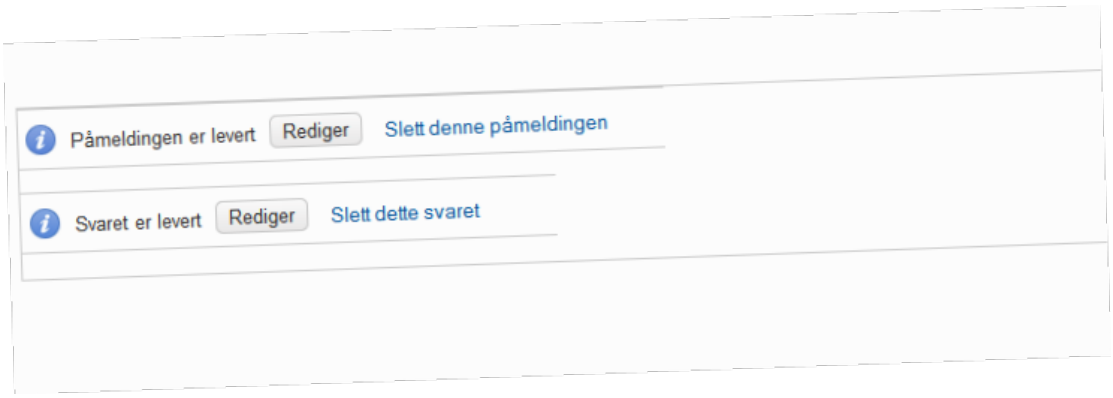
Risikovurdering av sikkert-nettskjema TSD 2.0

Version 1.0
2014-01-28

Espen Grøndahl
IT-sikkerhetssjef
UiO



1. Innledning

TSD 2.0 – tjenester for sensitive data er utviklet ved USIT ved UiO i perioden 2011-2014. Det baserer seg på en pilot TSD 1.0 som ble laget 2008-2011. Systemet har hatt som målsetning å lage et sikkert miljø som tilfredsstiller alle lovkrav med tanke på sikring av sensitive data. Det er primært sensitive forskningsdata innen helsesektoren som er i målgruppen, men også andre data som krever ekstra beskyttelse.

En del av denne løsningen er et system for å gjennomføre spørreundersøkelser og annen skjemabasert informasjonsinnsamling på nett. Dette dokumentet er første risikovurdering av denne løsningen, heretter kalt sikkert-nettskjema.

2. Bakgrunn

Tidlig i TSD 1.0 prosjektet så ble det fremmet av flere interessenter at en nettbasert løsning for innsamling av sensitive data ville medføre store besparelser for forskningsmiljøene ved UiO. Slik innsamling foregår fortsatt i stor grad via papirbaserte løsninger som koster store summer årlig bare i porto. I tillegg kommer etterbehandling som skanning, makulering osv.

USIT har i mange år hatt en løsning for slik datainnsamling, men den har primært vært benyttet for mindre sensitive data og den manglet flere egenskaper for kunne benyttes til for eksempel helsedata.

På bakgrunn av dette ble det utviklet en løsning basert på eksisterende løsning (nettskjema).

3. Avgrensing

Denne risikovurderingen er avgrenset til løsningen som omfatter autentisering til løsningen, innlegging av data og til den er overlevert inn til TSD 2.0. Den går ikke dypt i selve programvaren eller sikringen av servere og infrastruktur.

Dokumentasjon på sikring av server og database kan fremlegges for de med legitimt behov for dette. Kildekode for applikasjonen kan også fremlegges.

Analysen tar utgangspunkt i at bruker har tilgang på en tilstrekkelig sikret nettleser på nettbrett eller datamaskin.

4. Løsningsbeskrivelse

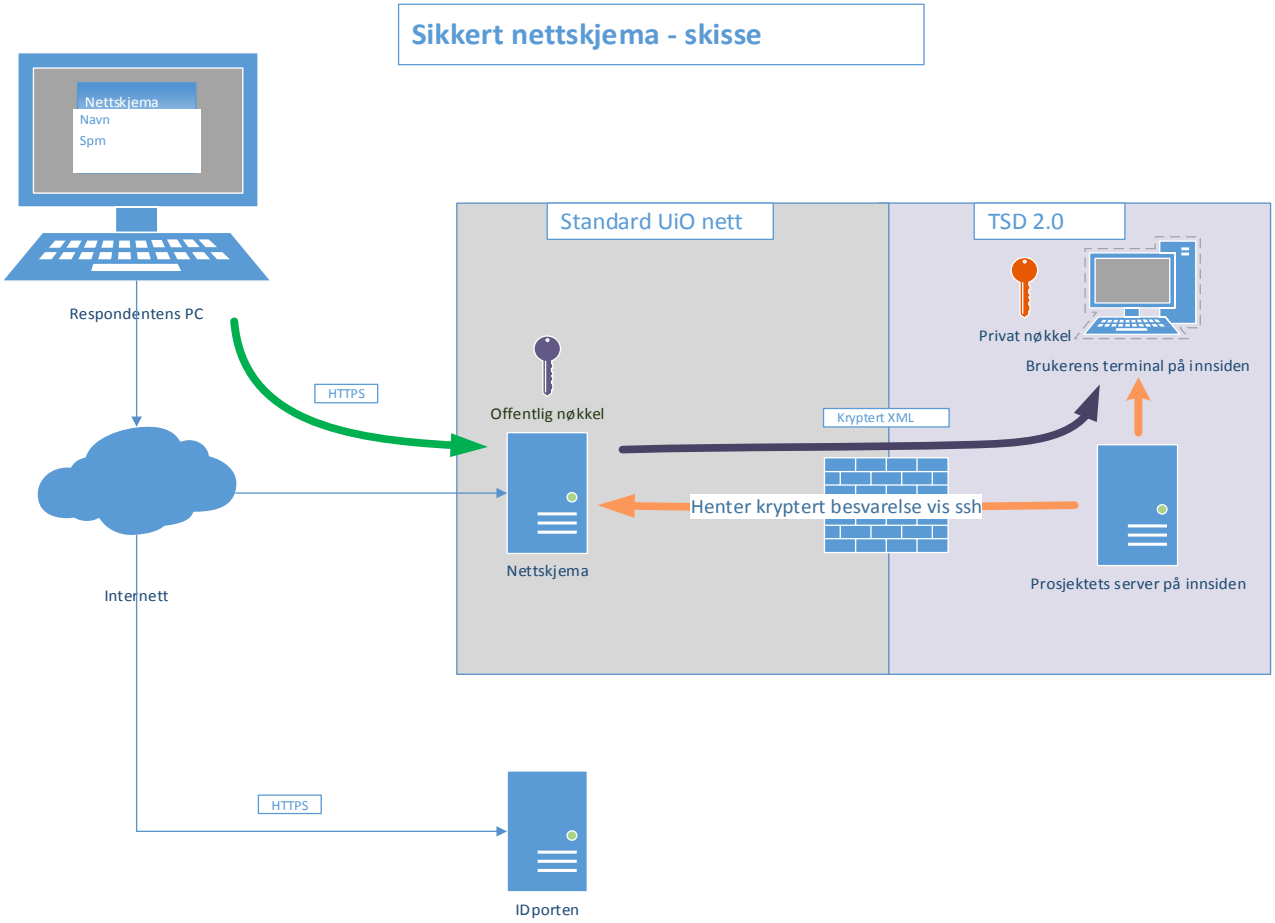


Fig 1. Sikkert nettskjema - skisse

4.1 Om nettskjema

Løsningen er basert på USITs nettskjema (http://www.uio.no/tjenester/it/applikasjoner/nettskjema/) dette er en web-basert løsning for å samle inn enkel skjemabasert informasjon. Brukere som har rettigheter til det kan opprette og redigere ett eller flere skjema og sende dette ut til respondenter som så svarer på skjemaet. Besvarelser kan enten være autentisert eller anonyme.

Besvarelsene fylles ut i brukerens nettleser, og går over https til applikasjonsserveren på USITs maskinrom. Der blir de lagret i en oracle base også på USITs maskinrom.

4.2 Om sikkert-nettskjema

Sikkert-nettskjema benytter samme maskiner og mekanismer som ordinært nettskjema, men med noen endringer og tillegg.

4.3 Autentisering

Sikkert-nettskjema er integrert med ID-porten slik at vi kan få autentisering opptil Nivå 4 jmf. " Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sector".

Det vil si at alle borgere i Norge med MinID (evt BankID, Commfides, ByPass) kan autentisere på en trygg og sikker måte for å levere besvarelser i sikkert-nettskjema.

4.4 Kryptering

Kryptering benyttes flere steder i løsningen. Først og fremst mellom klient og server ved at alle besvarelser og all autentisering skjer over HTTPS.

Videre så er hvert skjema i Sikkert-nettskjema utstyrt med en egen PGP-nøkkel. (http://en.wikipedia.org/wiki/Pretty_Good_Privacy#OpenPGP). Den offentlige delen av nøkkelen legges inn av den som oppretter skjemaet, mens den private beholdes på innsiden av TSD 2.0 løsningen, der nøkkelparet også genereres.

For hver besvarelse som legges inn vil data fra besvarelsen krypteres med den offentlige delen av nøkkelen og lagres på disk på serveren. Besvarelsene vil **ikke** lagres i oracle basen slik som de vil for "vanlig" nettskjema. Klartekst besvarelsen vil derfor aldri lagres hverken på web-server eller i database. Den vil finnes i minne på serveren i en veldig kort tidsperiode fra den er mottatt over HTTPS til den er kryptert. Kryptering skjer med bouncycastle java biblioteket (http://www.bouncycastle.org).

For ytterligere detaljer så kan kildekode og implementasjonsdetaljer fremvises.

4.5 Overføring til TSD 2.0

Besvarelsene lagres på et filområde på web-serveren og skjemaeier kan gjenkjennes basert på nøkkelens tilhørende epostadresse (prosjektnavn-basert) som kan ekstraheres fra den krypterte filen uten å dekryptere den. En automatisert jobb henter så disse besvarelsene inn til TSD 2.0 med SSH initsialisert fra innsiden av TSD. Besvarelsene vil flyttes til skjemaeiers prosjekt basert på prosjektnavnet som ekstraheres fra filen. Om noe skulle gå feil i denne overføringen så vil allikevel ingen andre enn den som sitter med privat-delen av PGP-nøkkelen kunne dekryptere besvarelsen.

Det finnes også en mekanisme som kan sende besvarelsene til en angitt e-post adresse. Besvarelsene vil da også være kryptert med PGP. Ved bruk av denne varianten så vil det kreve at mottakeren behandler besvarelsene sikkert etter dekryptering.

Det vil være automatiserte jobber som sikrer at besvarelser ikke blir liggende igjen på applikasjonsserveren.

4.6 Utvikling og kildekode

Utvikling av sikkert-nettskjema skjer i samme kildekode-base som resten av nettskjema. Her er det tilgangskontroll, versjonskontroll og full historikk. Nye versjoner testes grundig før utrulling, og evt. feil eller bevisste kode-endringer vil kunne avdekkes og spores.

4.7 Sikkerhetstesting

Det ble gjennomført en sikkerhetstest av nettskjema applikasjonen etter siste store oppgradering (nettskjema 3.0). Alle funn etter denne testen er lukket. Testrapporten kan fremlegges på forespørsel.

4.8 Driftsmiljø, infrastruktur og overvåking

Applikasjons-server og utviklings-servere er en del av USITs regulære driftsregime. Her er det sentral overvåking og logging. Maskinene oppdateres daglig med patcher fra RedHat og konfigurasjonsstyres med cfengine.

4.9 Bruk av sikkert-nettskjema for elektronisk signatur / samtykke

Pr 31/1-14 har sikkert nettskjema kun funksjonalitet for IDporten basert innlogging. Dette medfører at man har en sterk autentisering av personen som svarer på et skjema, men om man benytter dette til ”signering” eller samtykke så skal brukermiljø være klar over følgende :

1. En bruker kan hevde sin sesjon overtatt av andre etter initiell innlogging. Dette medfører at en bruker kan hevde at det ikke var hun/han som ferdigstilte skjema og trykket på ”submit”. (Pr 31/1-14 er det f.eks også slik AltInn opererer mtp å sende inn selvangivelse og endringer av skattekort, bekreftelse av navn på barn etc.
2. En bruker kan hevde at teksten som man samtykket til ved å trykke på ”submit” har blitt endret siden man faktisk leste den og trykket ”submit”. For å løse denne utfordringen må digital signatur innføres for hele nettskjema.

Tiltak for å bedre dette er som følger :

- For pkt 1 vil sikkert nettskjema innføre også muligheten til å be om en ekstra innlogging for å kunne få effektuert det å trykke på "submit" knappen. Med dette vil muligheten til å hevde at noen har overtatt en innlogget situasjon frafalle.
- For pkt 2 er sikkert-nettskjema av DiFi anbefalt å vente på deres totalløsning for digital signatur. Pr i dag er løsningen som f.eks Lånekassen har sydd sammen av DiFi produkt sammen med Signicat, og DiFi anbfalte oss ikke å gå denne veien enda ettersom teknologien er noe umoden. Det antas av DiFi har en komplett pakke for digital signatur i løpet av 2014, sikkert-nettskjema vil da jobbe mot å ta denne i bruk.

5. Beskyttelsesbehov

Data som skal lagres og behandles i løsningen har ulikt beskyttelsesbehov. En vurderer dette ofte langs tre akser. Konfidensialitet – sikring av at ingen andre enn de som har rettmessig behov får tilgang til data. Integritet – sikring av at data eller kode ikke manipuleres eller endres utilsiktet. Tilgjengelighet – sikre at data er tilgjengelig for rett person til rett tid.

Data som behandles i sikkert-nettskjema vil i første omgang kreve høy grad av konfidensialitet og integritet.. Dette er ikke tjenester som er beregnet for å høy tilgjengelighet – selv om de normalt vil være tilgjengelig 24x7.

6. Gjennomføring

6.1 Metode

Risikovurderingen er gjennomført etter metodikk som er benyttet ved USIT tidligere. Den er basert på tradisjonell innsamling av risikoelementer som vurderes ut fra sannsynlighet og konsekvens.

Risikovurderingen er gjennomført ved å ta utgangspunkt i den tekniske løsningen og dokumentasjon som finnes av denne – for så finne risikoelementer som kan true konfidensialitet, tilgjengelighet eller integritet for løsningen.

Risiko elementer er tatt frem vha. brainstorming og ut fra vurderinger som gjort i design og utviklingsfasen av løsningen. Disse er så vurdert ift. sannsynlighet og konsekvens.

6.2 Deltakere

Vurderingen er foretatt av:

Espen Grøndahl – IT-sikkerhetssjef

Gard O Sundby Thommasen – prosjektleder

7. Akseptkriterier

Sikkerhet vil alltid være en vurdering og en balanse mellom funksjonalitet og sikringstiltak. Noen risikoer vil være ønskelige å akseptere for å få en funksjonalitet som brukerne ønsker, og ikke minst – som gjør at brukerne benytter løsningen fremfor å velge å ikke forske eller velger å behandle data andre steder uten tilstrekkelig sikring.

I en løsning med så høy grad av sikkerhet som det vi tilstreber i TSD 2.0 så vil det være få risikoer vi vil akseptere. Løsningen skal ikke feile på en slik måte at sensitive data eksponeres utilsiktet. Hvis løsningen feiler så er det viktigere at løsningen opprettholder konfidensialitet og integritet enn tilgjengelighet. Dette vil bli vektlagt i vurderingen av risikoelementer.

Det er også foretatt noen avveiinger, vi kunne tilstrebet ende til ende kryptering ved å utføre krypteringen av informasjonen for eksempel med javascript på klienten. Vi valgte å ikke gjøre det fordi vi mener dette ikke pt. kan gjøres på forsvarlig måte, og at risikoen for at data kommer på avveie den korte tiden den finnes i minnet på serveren er veldig liten.

7.1 Vurderingsskala

Risikoelementene blir vurder på en skal fra 1-4 på sannsynlighet, og 1-4 på konsekvens. Der en 1 er lav sannsynlighet, eller liten eller ingen konsekvens. 4 er svært sannsynlig og svært alvorlig konsekvens.

7.2 Risikoelementer med et produkt mellom 1 og 4:

Dette er risikoelementer som kan aksepteres enten som de er, eller med enkle risikoreduserende tiltak eller rutiner.

7.3 Risikoelementer med et produkt mellom 4 og 8:

Dette er risikoelementer som må vurderes. De kan aksepteres i produksjon hvis de er kortvarige og risikoreduserende tiltak er planlagt.

7.4 Risikoelementer med et produkt mellom 8 og 16:

Dette er uakseptable risikoer. De vil i de fleste tilfeller bety produksjonsstans eller at det må kompenseres med manuelle kontroller og rutiner til risikoen er redusert.

8. Beskrivelse og vurdering av enkelt risikoelementer

Risikoelementene er listet opp i vedlagt excel fil. De er nummeret med løpenummer. Her følger en beskrivelse og vurdering av elementer som krever risikoreduserende tiltak eller spesiell oppmerksomhet.

Risiko 2 og 3 innbrudd på standard UiO servere

Webserver og utviklingservere er servere som er satt opp med standard UiO sikring. Denne ble fullstendig gjennomgått med innføring av RHEL 6.0 og vi anser den som meget god. Det er sentralisert logging med integritetskontroll av loggene, alle servere driftes og konfigurasjonsstyres med cfengine og endringer på kode i cfengine eller i programpakker må godkjennes av to personer før driftssetting.

Risiko 5 Risiko for at data i besvarelser lekker fra klienten som benyttes

Her er det viktig at man ved innsamling av sensitive data opplyser respondenten om at de selv er ansvarlige for sikkerheten (ormer og keylogging) på den fysiske enheten som benyttes til å gå inn via www og levere sin besvarelse.

9. Vurdering og videre oppfølging

Vi har ikke avdekket noen kritiske risiki som må lukkes før systemet kan gå i produksjon. Videre bør opsjon for påkrevd innlogging ved ”submission” implementeres omgående og digital signatur på plass når DiFi tilbyr dette som komplett tjeneste.

10. Konklusjon

Vår vurdering er at ved lukking av de alvorligste risikoelementene så er løsningen forsvarlig å ta i bruk for håndtering av svært sensitivt materiale. Løsningen er designet fra starten av for å ha meget høyt sikkerhetsnivå og det er ved produksjonsstart ingen kjente svakheter eller bakveier inn i systemet.

11. Tilhørende dokumentasjon

A. ”Whitepaper TSD 2.0”
B. Risikoelementer TSD 2.0 – sikkert nettskjema

Disse kan hentes på
http://www.uio.no/tjenester/it/forskning/sensitiv/Dokumenter/