

Pressepakke - Sikkerhetsportalen

Nærmere informasjon om Sikkerhetsportalen:

Hva er Sikkerhetsportalen?

Sikkerhetsportalen sørger for sikker dialog mellom brukeren og det offentlige på Internett, og at ingen andre får tilgang til dine opplysninger. Portalen åpner i tillegg for felles innlogging til flere offentlige tjenester, noe som for alvor vil komme innbyggerne til gode når flere etater og kommuner tar løsningen i bruk. For å få tilgang til tjenestene brukes et elektronisk identitetsbevis (elektronisk ID).

Sikkerhetsportalen gir også offentlige etater og virksomheter trygghet for at brukeren i andre ende er den han/hun utgir seg for å være, slik at det offentlige med sikkerhet kan utveksle informasjon med brukeren.

Hva skal Sikkerhetsportalen gjøre?

For at brukere enkelt skal kunne benytte offentlige tjenester som er tilgjengelig på Internett som krever sikkerhetshåndtering, har flere og flere etater og kommuner behov for å tilby sikker innlogging og sikker overføring av dokumenter til innbyggere, næringsliv eller andre offentlige instanser. Sikkerhetsportalen skal ivareta sikkerheten i denne typen dialog og samhandling.

Dersom alle etater og kommuner selv skulle lage sine egne sikre innloggingsløsninger, ville det bli svært kostbart for samfunnet. Det ville ta lang tid og bli uoversiktlig for brukerne.

Sikkerhetsportalen tilbyr et standardisert teknisk og visuelt grensesnitt som gjør det enklere for brukerstedene å tilby elektronisk identifisering i første omgang, og etter hvert også, elektronisk signering og kryptering av informasjon.

Hvorfor navnet Sikkerhetsportalen?

Sikkerhetsportalen er ikke en portal i vanlig forstand. Brukeren går som før direkte til de nettsidene som skal besøkes, og vil der møte noe av funksjonaliteten som tilbys av Sikkerhetsportalen.

Når en bruker benytter sikkerhetstjenester (for eksempel identifisering) vil Sikkerhetsportalen være involvert "i bakgrunnen", hvor den verifiserer at opplysningene brukeren gir er korrekte. Brukeren er avhengig av at opplysningene som oppgis "aksepteres" av Sikkerhetsportalen.

Hva er hovedgevinstene for brukerne?

At et brukersted (offentlig etat, kommune eller andre) benytter tjenester fra Sikkerhetsportalen vil gi flere gevinster for brukerne:

1. Sikkerhet mot innbrudd med bruk av falsk identitet. Personlige opplysninger (f.eks. inntekt, skatt, eiendom, helseopplysninger, etc.) skal bare være tilgjengelig for rette vedkommende.
2. Sikkerhet i kommunikasjon og oversendelse av dokumenter til/fra det offentlige.
3. Elektronisk saksbehandling og kommunikasjon mot brukere vil kunne gi høyere effektivitet i det offentlige og dermed resultere i lavere responstid overfor brukerne.
4. Borgere vil kunne få bedre og raskere service og saksbehandling fra det offentlige fordi ressurser frigjøres gjennom elektronisk innrapportering og saksbehandling.
5. Det vil bli mer lettvtint og raskere å bevege seg mellom ulike brukersted fordi det bare er nødvendig å logge seg inn én gang. Er man først innlogget (identifisert) f.eks. gjennom Altinn, vil man kunne gå til andre sider og benytte tjenester der uten å måtte logge seg inn på nytt.

Hva er hovedgevinstene for brukerstedene?

De viktigste gevinstene for brukerstedene er:

1. Det blir enklere og raskere å etablere sikkerhetsrelaterte tjenester via Internet når brukerstedene kan benytte standardiserte moduler i stedet for å utvikle dette fra bunn selv.
2. Det blir billigere å etablere sikkerhetsrelaterte tjenester når standardisert funksjonalitet kan kjøpes direkte fra Sikkerhetsportalen.
3. Økt bruk av elektroniske dokumenter vil kunne gi en mer effektiv og totalt sett raskere saksbehandling.

Hvem vil benytte Sikkerhetsportalen?

Både offentlige og kommunale virksomheter kan benytte tjenester fra Sikkerhetsportalen.

Fra 2006 skal alle statlige etater som anskaffer løsninger som krever bruk av elektronisk identitet benytte Sikkerhetsportalen, dersom de ikke har denne typen sikkerhetsløsninger fra før. Kommunene blir oppfordret til å bruke Sikkerhetsportalen.

Nærmere om teknologien bak Sikkerhetsportalen:

Hvilken teknologi er valgt?

BBS har valgt en løsning som skal være brukervennlig og enkel å integrere for brukerstedene. Det er satt fokus på bruk av åpne standarder og veletablert BBS-teknologi. Blant annet benyttes BBS sitt allerede etablerte driftsapparat. BBS Online, som er BBS sin kundeportal, vil bli brukt som administrasjonsportal (kundeweb) for brukerstedene og Brønnøysundregistrene.

Sikkerhetsportalen består av to hovedmoduler; en integrasjonsmodul som benyttes av brukerstedet, og en sikkerhetsserver som ligger hos leverandøren.

Integrasjonsmodulen består av eFactory Security Client levert av SPAMA, og SAML Affiliate Agent levert av Computer Associates. eFactory Security Client støtter autentisering og signering og kommuniserer med eFactory Security Server som er en del av sikkerhetsserveren via Web Services og HTTPS.

Sikkerhetsserveren som ligger hos leverandøren består av SPAMAs eFactory Security Server som tilbyr et standard grensesnitt mot ulike PKI løsninger. I tillegg består Sikkerhetsserveren av eTrust SiteMinder fra Computer Associates og har støtte for standard metoder for brukerautentisering og Single SignOn, samt innebygd støtte for SAML.

Hvordan sikres at flere PKI-leverandører kan benyttes?

Samtrafikk mellom de ulike PKI-leverandørene sikres ved å benytte SPAMAs eFactory Security Server, som er den ledende tjeneren for dette i det norske markedet. Viktig er det også at den enkelt kan utvides til å støtte andre PKI-løsninger. eFactory Security Client fra SPAMA vil sørge for enkel og sikker integrasjon for brukersteder.

For å sikre at overføring av informasjon tilknyttet funksjonen Single SignOn (SSO) mellom brukersteder følger etablerte standarder innenfor Federated Identity, har BBS valgt å benytte det markedsledende produktet eTrust SiteMinder fra Computer Associates. Bakgrunnen for dette valget er at denne leverandøren er den opprinnelige forfatteren av SAML og at de i dag er en av de fremste pådriverne for utbredelse av SAML, blant annet gjennom deres deltakelse i OASIS.

Hvordan bruker Ola Nordmann Sikkerhetsportalen?

Ola Nordmann vil benytte en offentlig tjeneste via Internett (det kan for eksempel være å levere flyttemelding). Hvordan foregår det?

1. Ola går til en offentlig etats nettsted, der blir han bedt om å identifisere seg for å få tilgang til en av tjenestene de tilbyr.
2. For å identifisere seg trenger han et elektronisk ID, som han kan få fra forskjellige utstedere av elektroniske sertifikat.
3. Når Ola bruker sin elektroniske ID, vil den offentlige etaten kontakte Sikkerhetsportalen for å sjekke om de oppgitte opplysningene er korrekte.
4. Sikkerhetsportalen sjekker da med utstederen av det elektroniske sertifikatet hvorvidt dette er gyldig, og hvilket sikkerhetsnivå sertifikatet gir tilgang til. Deretter sender Sikkerhetsportalen informasjon om identiteten og sikkerhetsnivå tilbake til den respektive etat.

Ola slipper inn, og kan utføre den ønskede tjenesten. Sikkerhetsjekken foregår i bakgrunnen, og Ola vil ikke merke det. Alt skjer i løpet av svært kort tid