Forord

Denne oppgaven er utført over en periode på 20 uker, ved Institutt for Datateknikk og Informasjonsvitenskap (IDI) ved Norges Teknisk-Naturvitenskapelige Universitet (NTNU).

Oppgaven inneholder et konsept for RFID-basert autentisering på internett, knyttet opp mot universelle profiler og en "Single Sign-on"-løsning.

En stor takk til veileder Claude Marie Davidsen for innspill og rettledning gjennom prosjektet.

Trondheim, 15. juni 2005

Kaare Kristian Lilleng

Sammendrag

Oppgaven beskriver et system for autentisering på internett ved hjelp av RFID-teknologi. Hensikten er å forenkle autentiseringsprosesser og øke brukervennligheten på internett.

RFID-teknologien blir gjennomgått ved å se nærmere på de ulike typene brikker, og hvordan RFID fungerer. Dagens situasjon blir analysert med en presentasjon av en del ulike autentiseringsmetoder som benyttes på internett i dag.

I det utarbeidete systemet autentiseres brukeren ved hjelp av en RFID-brikke montert på et vanlig bankkort. Datamaskinen har en RFID-leser som leser av kortet og kommuniserer med en sentralisert database som foretar autentisering av brukeren. Når brukeren senere besøker ulike nettsteder blir hun automatisk autentisert, og slipper dermed å huske på en rekke ulike brukernavn og passord. Denne autentiseringen skjer ved at nettstedet henvender seg til den sentrale databasen og får tilsendt autentiseringsinformasjon derfra.

En overordnet arkitektur basert hovedsaklig på sekvensdiagrammer illustrerer hvordan systemet er tenkt å fungere. Et rammeverk med oversikt over ulike aktører og hvilke krav som stilles til systemet er utarbeidet. En prototype basert på konstruerte skjermbilder viser hvordan sluttbrukeren vil oppleve systemet i bruk.

Videre arbeid kan være å foreta undersøkelser for å finne ut om markedet er interessert i et slikt system, samt å lage en implementasjon for å finne ut hvordan det vil fungere i praksis.

Innhold

Figurer

Kapittel 1

Innledning

I følge SSB hadde 60% av norske husholdninger tilgang til internett i 2004 (SSB, 2003).

På verdensbasis har minst hver tiende borger tilgang til nettet, noe som tilsvarer flere hundre millioner brukere (Digi.no, 2002).

En rekke nettsteder krever ulike former for identifisering før en får tilgang til alle, eller deler av, de tjenestene nettstedet tilbyr. Den vanligste metoden, som baserer seg på brukernavn og passord, krever at brukeren oppgir et tidligere valgt eller tildelt brukernavn med et tilhørende passord. Ettersom de fleste benytter seg av mange nettsteder, medfører dette av hver enkelt bruker må huske på, eller på andre måter oppbevare, en økende mengde med brukernavn og passord.

Det en utfordring for brukervennligheten at nettsamfunn, nettbutikker, banker, diskusjonsfora og så videre krever brukernavn og passord, eller annen tungvindt autentisering, før brukeren får tilgang. Problemet med å holde rede på et utall forskjellige innloggingsopplysninger får sannsynligvis potensielle brukere til å begrense seg med tanke på hvor de velger å registrere seg.

Den desentraliserte oppbevaringen av brukerinformasjon hos hvert enkelt nettsted med egen brukerdatabase medfører at opplysningene over tid vil bli mer upålitelige. Om en bruker flytter til et annet sted av landet og får en ny adresse, er det liten sjanse for at hun logger seg inn på samtlige nettsteder hun er registrert på for å oppdatere adresseinformasjonen sin. Dermed vil nettstedenes databaser etterhvert degenerere og fylles opp med mangelfull og utdatert informasjon.

Ved å benytte en sentralisert håndtering av personinformasjon som nettstedene kan benytte seg av for å hente ut aktuelle data vil slike problemer kunne unngåes. Brukeren får bare ett enkelt sted å forholde seg til når personinformasjon skal oppdateres, noe som ønker sannsynligheten for at brukerdataene faktisk vil holdes oppdatert.

Oppgaven presenterer et system for autentisering på internett ved hjelp av RFID-teknologi. Med bruk av en Single Sign-On-løsning og en sentralisert profildatabase er hensikten å gi en verdiøkning for sluttbruker, ved at autentiseringsrutiner og administrering av personinformasjon forenkles.

1.1 Oppgaven

"Identifikasjon på web er i dag i stor grad basert på brukernavn- og passordbasert innlogging. For brukeren betyr dette at det er nødvendig å holde rede på en stadig økende mengde brukernavn og passord. En løsning på dette kan være å knytte identifikasjonen mot en RFID-brikke brukeren har med seg. Oppgaven går ut på å utrede konsekvenser og forenklinger med et system som baserer seg på RFID-teknologi for identifisering og skissere et rammeverk/arkitektur. En enkel prototype skal utarbeides."

1.2 Oppgavens fokus

Målet er å tilby et portabelt, brukervennlig og sikkert system for autentisering på World Wide Web. Portabilitet er nødvendig, fordi et system som bare kan brukes på én datamaskin vil medføre betydelige begrensninger i forhold til dagens brukernavn/-passord-metode. Brukervennlighet er påkrevet for at det i det hele tatt skal være interessant å ta i bruk systemet. God sikkerhet er nødvendig for at systemet skal oppnå tillit og aksept hos brukerne.

Konsekvenser og forenklinger med et slikt system drøftes, og et rammeverk og en overordnet arkitektur presenteres. En ren autentiseringsløsning basert på RFID gir ikke en tilstrekkelig verdiøkning for sluttbruker, og systemet knyttes derfor også opp mot universelle profiler og en Single Sign-on-løsning.

1.3 Oppgavens struktur

Kapittel 2 beskriver ulike måter å autentisere seg på internett. De vanligste måtene gjennomgåes, og et scenario viser noen av utfordringene med dagens autentiseringsmetoder.

Kapittel 3 omhandler RFID-teknologien generelt, og introduserer noen begreper relatert til RFID. Metoder for kommunikasjon på internett beskrives.

Kapittel 4 presenterer konseptet MyID. Kapittelet drøfter blant annet ulike steder å plassere RFID-brikken, samt håndteringen av den universelle profilen og kommersialiseringen av systemet.

Kapittel 5 inneholder kravspesifikasjon med Use Cases, overordnet arkitektur og oversikt over flyten i systemet.

Kapittel 6 gir noen eksempler på hvordan systemet er tenkt å fungere i praksis ved hjelp av konstruerte skjermbilder.

Kapittel 7 gir en oversikt over diverse svakheter med oppgaven.

Kapittel 8 inneholder oppgavens konklusjon og forslag til videre arbeide.

1.4 Sentrale begreper

En del begreper som er sentrale i oppgaven avklares her. Andre forkortelser og mindre sentrale begreper finnes i ordlisten.

MyID
MyID er et konsept som gjør det mulig for butikker å tilby personaliserte opplevelser og tilbud. - *Ved å kombinere data fra kundens besøk i den fysiske butikken og kundens kjøp over nettet, kan butikkene ved hjelp av universelle profiler tilby en individuelt tilpasset og personalisert opplevelse.* (Lilleng, 2004).

I denne oppgaven vil konseptet MyID utvides med en autentiseringsmulighet og "Single Sign-on" på World Wide Web.

RFID
RFID (Radio Frequency IDentification) går ut på å identifisere objekter ved hjelp av radiobølger. RFID beskrives nærmere i kapittel 3

Bruker
En bruker er en person som sitter med en installasjon av MyID-systemet. Hun har en datamaskin med MyID-programvare installert, og en tilkoblet RFID-leser.

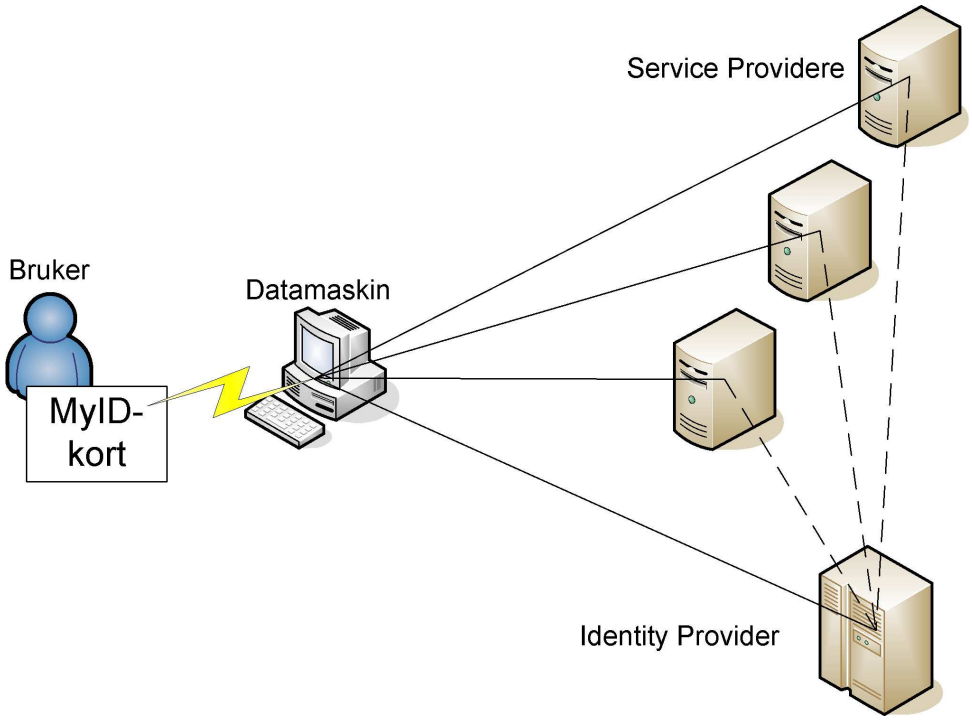
Identity Provider
En Identity Provider (IDP) er i denne oppgaven den sentrale databasen som inneholder brukerens personinformasjon, samt den som foretar autentisering av brukeren.

Service Provider
En Service Provider (SP) tilbyr en eller annen tjeneste til brukeren. SP har gjerne ett eller flere beskyttede områder som krever autentisering før tilgang gis. Ved hjelp av IDP kan SP tilby tilgang til sine beskyttede områder, uten at brukeren på forhånd har registrert seg med sine personalia hos den aktuelle SP. Eksempler på Service Providere kan være nettbutikker, diskusjonsfora og nettbanker.

Begrepene Service Provider og Identity Provider er hentet fra The Liberty Alliance Project (Project Liberty, 2005). En grundigere gjennomgang av de tre begrepene bruker, IDP og SP finnes i avsnitt 4.1. Figur 1.1 viser sammenhengen mellom bruker, Identity Provider og Service Providere i denne oppgaven.

Single Sign-on
Single Sign-on (SSO) er en mekaniske som skal gjøre det mulig for en bruker å autentisere seg én gang, for så å få tilgang til alle andre steder hun har tilgang til, uten å måtte autentisere seg på hvert enkelt av dem. Single Sign-on muliggjør et av hovedpoengene med oppgaven, det å forenkle autentiseringsprosessene på internett (OpenGroup.org).

Universell profil
I denne oppgaven er en universell profil en samlig med persondata lagret hos en sentral tjener (IDP). Profilen inneholder typiske personalia som navn, adresse, alder og så videre. Den kan også inneholde data som for eksempel kjøpshistorikk, personlige interesser og klesstørrelser. Avsnitt 4.2 går nærmere inn på universelle profiler.



Figur 1.1: Bruker, IDP og SP i sammenheng.

Kapittel 2

Dagens situasjon

I dag brukes det en rekke metoder for å identifisere seg på nettet. World Wide Web (WWW) var i utgangspunktet konstruert for å vise enkel tekst og grafikk, og hadde ikke innebyggete mekanismer for sikker autentisering. Dette har senere blitt delvis løst med ulike tillegg og utvidelser, men disse inneholder hver for seg en del ulemper som begrenser brukervennligheten. De følgende avsnittene gir en kort gjennomgang av de ulike metodene.

2.1 Brukernavn og passord

En svært utbredt form for identifisering er brukernavn og passord. Normalt registrerer brukeren seg ved første besøk på nettstedet og velger, eller får tildelt, et brukernavn og passord. Dette lagres i nettstedets database, enten kryptert eller ukryptert, og ved senere besøk bruker den besøkende brukernavnet og passordet for å få tilgang til nettstedet. Figur 2.1 viser et eksempel på en innloggingsboks.

En utfordring knyttet til denne måten å gjøre det på, er at nettstedet ikke har noen garantier for at personinformasjonen brukeren legger inn ved første gangs registrering er korrekte. Dette betyr at man kan benytte en annens navn under registreringen, og på den måten utgi seg for å være en annen. I tillegg er brukeren nødt til å huske brukernavn og passord på alle nettsteder hun registrerer seg på, noe som i lengden blir mye informasjon å holde rede på. For å bøte på dette kan brukeren benytte samme brukernavn og passord på samtlige nettsteder, men dette er en usikker praksis som vil få konsekvenser dersom uvedkommende får tak i bare én av databasene.

Det er noen fordeleler med brukernavn/passord-metoden, blant annet at det er svært enkelt å bruke, og de fleste kjenner til hvordan det fungerer. Det er også relativt uproblematisk å opprette flere kontoer dersom det av eller annen grunn skulle være nødvendig.

Dagens nettlesere har som regel mulighet for å lagre brukernavn og passord, slik at dette blir automatisk fyllt ut når brukeren navigerer til den aktuelle siden. Dette er

forenklende system som har noen betydelige svakheter. Dersom brukeren for eksempel installerer operativsystem på nytt eller bytter nettleser forsvinner alle de lagrede brukernavnene og passordene. Portabiliteten er også ikke-eksisterende, bruker man en annen datamaskin må passordene likevel hentes frem fra hukommelsen. I verste fall kan man risikere å be nettleseren på en fremmed maskin huske sitt brukernavn og passord ved et uhell, slik at neste person som bruker den kan logge inn med en annen persons konto.

Figur 2.1: Eksempel på en innloggingsform (PSData, 2005)

2.2 Cookies

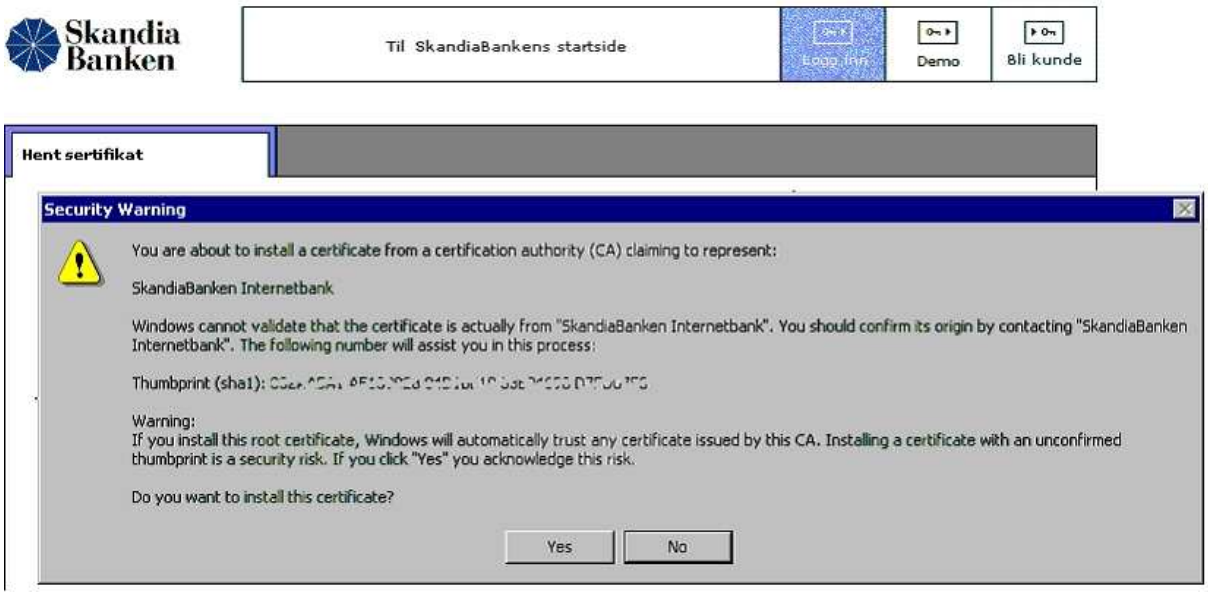
En cookie er en liten informasjonskapsel, lagret som en fil på brukerens datamaskin. En typisk bruk for cookies er å lagre brukernavn og passord, slik at brukeren ikke trenger å taste inn dette ved hvert besøk på nettstedet. Bruken av cookies kan forenkle brukernavn/passord-metoden, men innebærer en risiko i det at hvem som helst som bruker maskinen vil kunne benytte seg av cookien for å komme seg inn på nettsteder. I tillegg er det en risiko i det hele tatt å ha lagret innloggingsinformasjon på datamaskinen, selv om cookies også kan krypteres. Det største problemet med cookies er imidlertid at de også kan brukes for å holde rede på mer enn brukernavn, de kan også inneholde detaljert informasjon om hvordan brukeren har benyttet seg av nettstedet, og følges opp med målrettet reklame, uten at brukeren har gitt sitt samtykke til en slik overvåkning (Wilkens, 1999).

```
hardwareanonlogin
-1
forum.hardware.no/
1536
2305363968
29695767
284732768
29622342
*
hardwaremember_id
16291
forum.hardware.no/
1536
1156701824
```

Figur 2.2: Utdrag fra en cookie, laget av forumet på Hardware.no

2.3 Sertifikat

Sertifikater gir en sikkerhet utover rent brukernavn og passord. Et sertifikat er informasjon utstedt fra nettstedet og lagret på brukerens datamaskin. For å få tilgang til nettstedet kreves det både sertifikat, brukernavn og passord. Skandiabanken er et av flere nettsteder som benytter seg av dette systemet. Sertifikatet må hentes ned til og lagres på datamaskinen først, før det gies tilgang til banken. På den måten vil for eksempel ikke et angrep basert på tilfeldige personnummer og PIN-koder fungere. For å få lastet ned sertifikatet må det tastes inn et engangspassord som sendes via SMS til brukerens mobiltelefon. Ulempen med sertifikater er at det må lastes ned til hver datamaskin man skal logge inn på. Hvis hvert nettsted bruker et sertifikat blir det etter hvert svært tungvindt, og portabiliteten blir dårlig. Figur 2.3 viser et sertifikat fra Skandiabanken.no.



Figur 2.3: Sertifikatnedlasting fra Skandiabanken.no

2.4 Microsoft InfoCard

Microsoft lanserte i 2001 en tjeneste kalt ”Passport”, som skulle tilby en felles innlogging til mange nettsteder. Det var dog liten respons fra markedet, og Passport har mer eller mindre blitt faset ut fra markedet. Microsoft er nå i gang med en ny løsning, kalt ”InfoCard”, der data lagres på brukerens datamaskin fremfor hos en sentral database (Digi.no, 2005). Systemet skal blant annet støtte Liberty Alliance sine spesifikasjoner, mer om disse i avsnitt 4.2.1. En betydelig ulempe med å lagre data på en lokal datamaskin er at portabiliteten blir dårligere enn ved lagring i en sentral database, fordi brukeren dermed ikke har tilgang på sitt personlige ”InfoCard” på andre maskiner enn den hun i utgangspunktet har lagret ”InfoCard’et” på. Dermed får hun ikke ut-

nyttet mulighetene i systemet i de tilfellene at hun benytter andre datamaskiner enn sin egen.

2.5 Smartkort og andre eksterne enheter

I stedet for, eller i tillegg til, å benytte seg av en autentisering basert på brukernavn og passord, eller informasjon lagret på datamaskinen, kan det benyttes eksterne, fysiske enheter som ekstra sikkerhet. Norsk Tipping benytter seg for eksempel av en smartkortløsning, der kortet må være plassert i en kortleser koblet til datamaskinen før brukeren får tilgang til sine personlige spillesider hos selskapet.

Postbanken benytter seg av en annen løsning, en "kodekalkulator", der brukeren taster inn en firesifret PIN-kode og får frem en autentiseringskode som brukes for å logge inn i nettbanken. Andre nettbanker igjen bruker et kodekort, der det står en liste med ulike PIN-koder, og brukeren får beskjed om å benytte en bestemt av disse for innlogging.

Felles for disse løsningene er at de tilbyr en ekstra sikkerhet, ved at tilgang ikke gis uten av man er i besittelse av den fysiske gjenstanden.

En RFID-basert løsning vil havne i samme kategori som smartkort og kodekalkulatorer, det er en ekstern gjenstand som kreves før tilgang gis. Forskjellen er at RFID er trådløst. Dermed slipper brukeren å fysisk koble til et smartkort eller lete frem en kodekalkulator og huske PIN-koden. Trådløs teknologi gjør det lettere for brukeren å alltid bære med seg RFID-brikken, noe som igjen fører til økt portabilitet.

2.6 Scenario

Kari Nordmann er en aktiv internettbruker. Hun har brukerkontoer på en lang rekke nettbutikker, hun benytter internettbank og -forsikring, og hun er registrert på diverse diskusjonsfora. En typisk morgen for Kari kan med dagens systemer for autentisering arte seg slik:

"Dagens første besøk går til hardware.no, der hun har lagt inn et innlegg med spørsmål angående kjøp av ny datamaskin. Hardware.no benytter cookies, slik at det ikke er nødvendig å taste inn brukernavn og passord hver gang. Når hun klikker på lenken for å se de trådene hun følger med på, får hun opp en rekke innlegg hun ikke kjenner igjen. Hun oppdager da at hun faktisk er logget inn som sin ektemann, som brukte datamaskinen kvelden i forveien. Hun logger seg ut, og inn igjen med sitt eget brukernavn og passord.

Kari har mottatt flere svar på innlegget sitt, og et av disse har en direktelink til Komplett.no, med et ferdig oppsatt forslag til maskin. Hun klikker på tilbudet, og blir videresendt til Komplett.no sine nettsider. Prisen er oppgitt, men for å finne fraktkostnader må hun logge seg på med brukernavn og passord. Hun husker at hun tilfeldigvis

har brukt samme brukernavn som på Hardware.no, og logger seg inn for å få rede på totalprisen med frakt.

- Datautstyr er sannelig dyrt, tenker hun, best å sjekke hvor mye penger jeg har på konto. Hun åpner et nytt nettleservindu og åpner postbanken.no. For å logge inn må hun skrive inn personnummer, samt en kode fra Postbankens kodekalkulator. Søren, tenker hun, hvor la jeg nå den.. Etter et par minutters intens leting gjennom skuffene i skrivebordet finner hun den, under en bunke med regninger.

For å få opp koden som kreves for å kunne å logge seg inn må hun først taste inn en PIN kode på kalkulatoren. Heldigvis har Kari god hukommelse, så det går uten problemer. På saldooversikten ser Kari at shoppingturen på byen i går har gjort et dypt innhogg i kontoen, så PC-kjøpet må utsettes til etter neste lønning. Hun bestemmer seg for å sjekke nattens mottatte e-post, og navigerer seg frem til webmail-siden Hotmail.com, og logger inn med riktig brukernavn og passord. Oi, mail fra bokklubben, ny bok. - Den har jeg jo allerede lest, tenker Kari, og klikker på lenken for å avbestille. Hun blir videresendt til bokklubben.no, og må logge inn med brukernavn og passord for å komme inn på avbestillingssiden."

I løpet av relativ kort tid har Kari måttet taste inn fire ulike brukernavn med tilhørende passord, blitt autentisert som en annen person, og generert én kode med kodekalkulatoren. MyID-konseptet som presenteres i kapittel 4 har som mål å forenkle Karis hverdag på internett ved å fjerne de lite brukervennlige løsningene hun gikk gjennom i dette scenarioet.

Kapittel 3

Teknologien

Det sies at røttene til det vi i dag kjenner som RFID går tilbake til andre verdenskrig. De krigende parter benyttet seg av radaren, som var oppfunnet få år tidligere av den skotske fysikeren Sir Robert Alexander Watson-Watt, for å oppdage fly lenge før de var synlige med det blotte øye. Et problem som oppstod var å finne ut om det var egne eller fiendtlige fly som var på vei. Tyskerne oppdaget at dersom piloten manøvrerte flyet til å vifte med vingene, endret det reflekterte radiosignalet seg, og bakkemannskapet kunne på den måten skille mellom egne og fiendtlige fly.

Wattson-Watt fortsatt arbeidet med radiobølger, og i et hemmelig prosjekt utviklet britene et aktivt system for identifisering. På hvert fly ble det plassert en radiosender, som begynte å sende når den mottok et bestemt signal. RFID virker på samme måte: Et signal sendes til en transponder som vekker opp databrikken og får den til å sende et signal tilbake, typisk det unike identifikasjonsnummeret som ligger lagret på brikken.

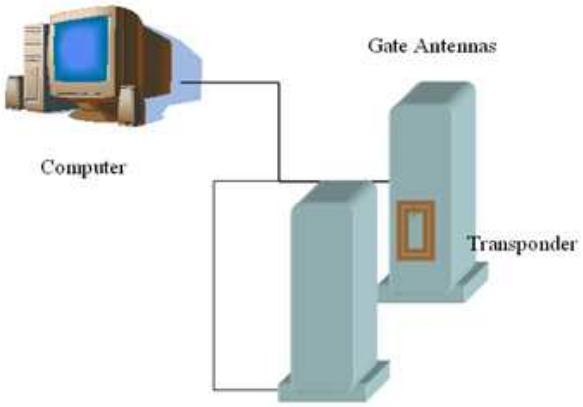
I tiårene etter krigen fortsatte utviklingen, og kommersielle krefter begynte å se nærmere på ulike bruksområder for teknologien. Et velkjent bruksområde er tyverisikring av varer, som vanligvis baserer seg på en 1-bit brikke. Når varen betales for føres varen over en innretning som endrer bit'en fra på til av. Dersom dette ikke skjer vil alarmen gå når kunden passerer gjennom sensoren på vei ut (RFIDJournal, 2003).

En moderne RFID-brikke har vanligvis lagret et lengre identifikasjonsnummer eller annen informasjon, avhengig av bruksområde. Slike brikker er allerede tatt i bruk på en rekke områder, for eksempel til bompengeinnkreving, merking av dyr og som betalingsmiddel for drivstoff.

De følgende avsnittene går igjennom RFID-teknologien, hvordan brikkene fungerer og standardisering knyttet til RFID. I tillegg inneholder avsnitt 3.6 en oversikt over kommunikasjonsmetodene SOAP, SAML og Web Services.

3.1 RFID-teknologien

Begrepet RFID (Radio Frequency IDentification, radiofrekvensidentifisering) omfatter systemer som via radiobølger kan identifisere et objekt. Selve RFID-brikken er som regel en mikrochip med et lagret identifikasjonsnummer, koblet til en antenne. Tilsammen kalles dette ofte en tag. Når taggen får tilført energi via radiobølger, sender den ut sin identifikasjon til leseren, som fanger opp signalet. Leseren omgjør signalet til et fornuftig format og sender det videre til en datamaskin for behandling. (Lilleng, 2004)



Figur 3.1: RFID-leser koblet sammen med en datamaskin (RFIDAsia, 2003)

3.2 RFID-brikken

En RFID-brikke (tag) er en elektronisk krets koblet sammen med en antenne. På kretsen kan det lagres informasjon, og denne informasjonen kan ved hjelp av antennen sendes til omverdenen når taggen aktiveres. Taggene finnes i ulik størrelse og fasong, med varierende rekkevidde og kompleksitet. Tidligere var taggene forholdsvis store og dyre, men de siste årene har både størrelse og pris minsket betraktelig. Pr april 2004 kostet én tag 20 US cent (RFIDJournal, 2004), og prisene er på vei nedover. Likevel er det flere som mener at prisen ikke vil nå 5 cent før i 2008 eller senere (RFIDJournal, 2004). 5 cent regnes som grenseverdien før RFID kan rulles ut i massivt omfang, også på lavkostprodukter. For denne oppgaven er det ikke veldig relevant om prisen for brikkene er 5 eller 50 cent, men prisutviklingen gir en indikasjon på når RFID kan forventes å være utbredt i mye større skala enn i dag.

Utviklingen gjør det uansett mer og mer aktuelt å merke enkeltprodukter med hver sin tag, selv om det foreløpig ikke er lønnsomt på de aller billigste varene. Produkter som elektronikk, kosmetikk, tekstiler og smykker er derimot aktuelle kandidater for slik merking. Ved å merke hvert produkt individuelt kan det være enklere å forebygge tyveri og annet svinn, og vareopptelling kan utføres med et tastetrykk, fordi systemet til en hver tid har kontroll på hvor hver enkelt vare befinner seg.

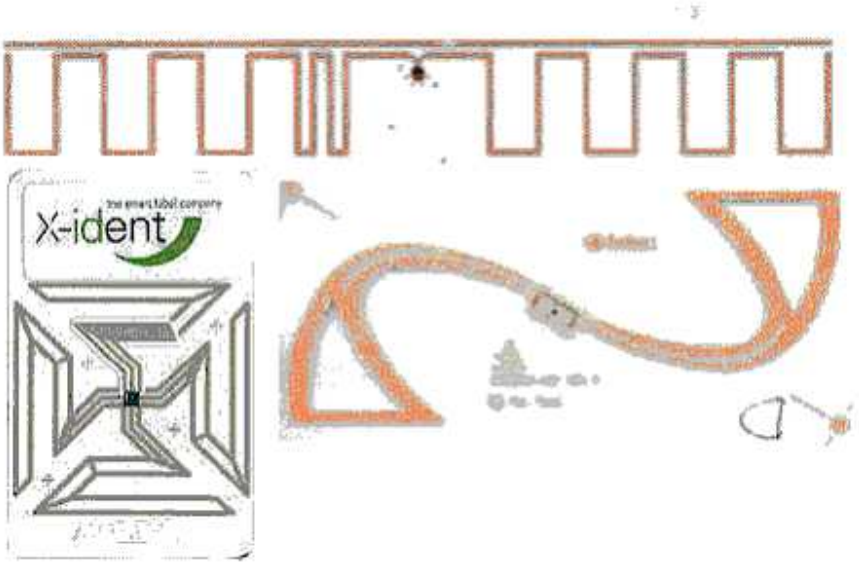
I hovedsak eksisterer det to typer tagger: Aktive og passive. Aktive tagger har sin egen strømforsyning (som regel et lite batteri), og kan inneholde forholdsvis store mengder med data. En passiv tag har ingen strømforsyning, og aktiveres først når den kommer inn i et magnetfelt som induserer strøm i taggen.

3.2.1 Aktive tagger

Aktive tagger har god rekkevidde, opp mot 100 meter, og hastigheten på overføringen er høyere enn på passive tagger. En stor ulempe med en aktiv tag er batteriet, som ikke er evigvarende. Levetiden avhenger av hvor ofte den må sende ut informasjon, men før eller siden går den tom for strøm, og batteriet må byttes eller taggen kasseres. Aktive tagger er også større og dyrere enn passive tagger, noe som gjør dem uegnet for lavkostvarer.

3.2.2 Passive tagger

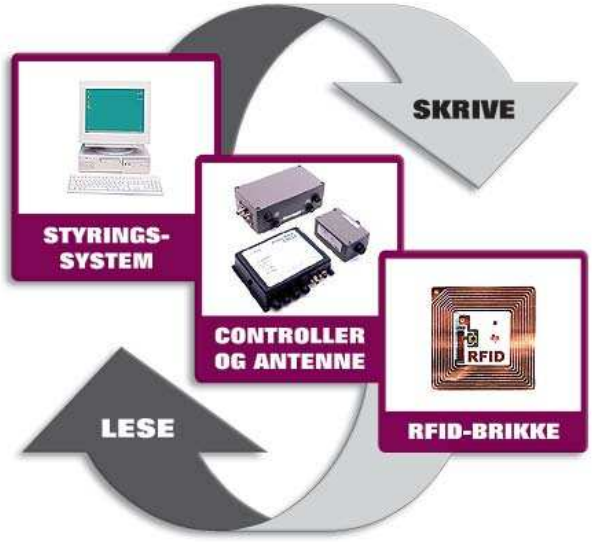
Sammenliknet med aktive tagger har passive tagger kortere rekkevidde og mindre lagringskapasitet, men til gjengjeld er de ikke avhengig av en egen strømforsyning. De får tilført energien de behøver gjennom elektrisitet indusert av magnetfeltet avleseren setter opp. På grunn av at en passiv tag ikke er avhengig av et batteri er den teoretiske levetiden svært lang. Derfor er passive tagger de mest interessante når det kommer til merking av varer og andre lavkostoppgaver. På grunn av den gode levetiden og lave kostnaden vil passive tagger egne seg godt til bruk i MyID-konseptet.



Figur 3.2: Noen RFID-tagger (SpyChips.com, 2004)

3.2.3 Kommunikasjon mellom tag og leser

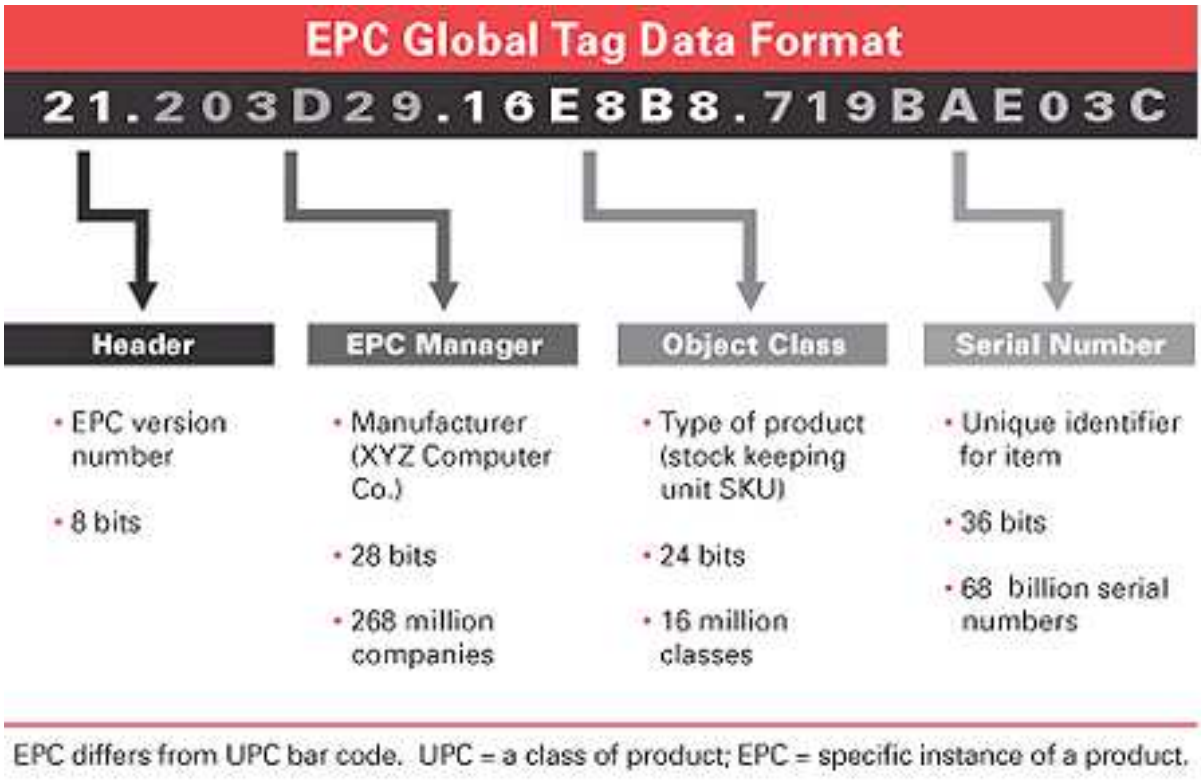
Dagens RFID-brikker aktiveres ved at leseren, via sin antenne, sender ut radiobølger på riktig frekvens. Det dannes et magnetisk felt mellom antennen i leseren og antennen koblet til mikrobrikken. Ved induksjon utnyttes dette feltet til å produsere elektrisk energi som "vekker" brikken. Brikken svarer med å sende ut informasjonen den inneholder, som oppfanges av leseren og omgjøres til fornuftige data. Disse dataene, som regel det unike identifikasjonsnummeret, sendes videre til datasystemet for behandling.



Figur 3.3: RFID-system (PSI Norge, 2003)

3.3 RFID-standarder

Electronic Product Code (EPC) er en sammenslutning mellom Uniform Code Council i USA og European Article Numbering i Europa. EPC er den største standardiseringsorganisasjonen innenfor RFID, og er bredt akseptert av markedet (EPC, 2005). Figur 3.4 viser oppbygningen av identifikasjonsnummeret som hver brikke utstyres med. Det er satt av plass til å identifisere produsent, produkttype og det individuelle produktet. Selv om det ikke er en absolutt nødvendighet å forholde seg til denne standarden i MyID-systemet, er det likevel ingen grunn til ikke å gjøre det. Ved å holde seg til en standard kan bruksområdene tenkes utvidet utover konseptet foreslått i denne oppgaven, for eksempel til betalingsløsninger i vanlige forretninger, erstatning for passkontroll på flyplasser og så videre.



Figur 3.4: EPC standarden (Symbol.com, 2004)

Dersom bare "Serial Number" delen av EPC standarden benyttes til å gi ut identitetsnummer vil det være plass til 68 milliarder personer i systemet. Dette er tilstrekkelig i uoverskuelig fremtid, men det medfører at det er forholdsvis enkelt å gjette hvilke nummer som er i bruk. Alternativt kan både "Object Class" og "Serial Number" delen kombineres, noe som gir 60 bit lange identitesnummer og over ti millarder milliarder kombinasjoner.

3.4 Fordeler med bruk av RFID

I prinsippet kan konseptet gjennomføres helt uten bruk av RFID. RFID-brikken kunne erstattes med et vanlig smartkort, som allerede finnes på markedet, ref. avsnitt 2.5. Det er likevel én sentral fordel med RFID-teknologien som gjør at denne egner seg bedre enn et smartkort: Den er trådløs. Stadig mer av det elektroniske utstyret vi benytter oss av i hverdagen benytter trådløs teknologi. Tastatur og mus til datamaskinen, trådløse høyttalere, trådløs kommunikasjon med BlueTooth og Wireless LAN, trådløs overføring av lyd og video fra datamaskinen til TV, og så videre. En trådløs løsning er dermed fremtidsrettet, samtidig som den er brukervennlig ved at man unngår å fysisk måtte finne frem smartkortet og plassere det i en avleser. En slik fordel øker portabiliteten, i og med at brukeren heller ikke glemmer å ta med seg kortet når hun forlater maskinen. RFID-brikken kan bæres med rundt overalt, på et bankkort i lommeboken, integrert i mobiltelefonen eller som et smykke rundt halsen.

3.5 Utfordringer knyttet til RFID

Det er noen utfordringer knyttet til å benytte en RFID-brikke i forbindelse med autentisering. Hvilken som helst avleser i nærheten vil kunne oppfange kortet, og hente ut identifikasjonsnummeret som ligger på brikken. Kombinert med et "Brute Force"-passordsøk kan uvedkommende få tilgang til andres brukerkontoer. Den potensielt store mengden identifikasjonsnummer som EPC standarden tillater, vanskeliggjør en slik taktikk, men umuliggjør den ikke.

Duplisering, det vil si at noen fanger opp informasjonen på et kort og reproduserer informasjonen, kan medføre misbruk om de ondsinnede får tak i passordet knyttet til brukerkontoen. ExxonMobile sitt trådløse betalingssystem for bensin, SpeedPass, er allerede knekt (Carbuyersnotebook.com, 2005) og et RFID-basert autentiseringssystem må derfor konstrueres slik at duplisering og kodeknekking blir så vanskelig som mulig.

En RFID-leser for hjemmebruk kan koste opp mot 300 dollar. Figur reffig:rfidleser viser en leser fra selskapet iAutomate.com til en pris av 299 dollar (IAutomate.com, 2005). Denne kostnaden er forholdsvis høy, og kan medføre at mange vil vegre seg for å ta i bruk RFID-teknologi.

Figur 3.5: RFID-leser for hjemmebruk (IAutomate.com, 2005)

3.6 Kommunikasjon på nettet

De følgende avsnittene gir en kort oversikt over de ulike kommunikasjonsteknologiene som er benyttet i MyID-konseptet. Ved å benytte standardiserte protokoller og teknologier ivaretas fremtidige utvidelsesmuligheter og oppgraderinger, i tillegg til kompatibilitet med dagens datasystemer.

3.6.1 HTTP

HTTP (HyperText Transfer Protocol) er den mest brukte metoden for å overføre informasjon på World Wide Web, og ble opprinnelig utviklet for å tilby en måte å publisere og lese HTML-sider. HTTP er en "henvendelse/svar" protokoll mellom klienter og tjenere. En HTTP-klient, for eksempel en vanlig nettleser, lager en henvendelse ved å etablere en TCP-forbindelse til tjeneren. Tjeneren mottar denne, og svarer ved å sende tilbake den ønskede informasjonen (Wikipedia.org, 2005)

Kommunikasjonen mellom en Service Provider og brukeren er i MyID-konseptet lagt opp til å gå via HTTP, som alle nettlesere er laget for å håndtere.

3.6.2 SOAP

SOAP er en XML-basert kommunikasjonsprotokoll og et format for interapplikasjonskommunikasjon. SOAP ble opprinnelig utviklet av Microsoft og Userland software, men har utviklet seg videre og øker i popularitet og bruk. SOAP er sett på som ryggraden til neste generasjons kryss-plattform, kryss-språklige, distribuerte applikasjoner: Webtjenester (Web Services). SOAP tilbyr en enkel mekanisme for å utveksle strukturert og typet informasjon mellom klienter i desentraliserte og distribuerte omgivelser ved å bruke XML (W3C.org, 2004).

Hensikten med å benytte SOAP er å oppnå en standardisert, formell og utvidbar kommunikasjon mellom IDP og SP basert på XML.

3.6.3 SAML

SAML (Security Assertion Markup Language) er et XML-rammeverk for å utveksle autentiserings- og autoriseringsinformasjon. SAML beskriver forskjellige typer meldinger og standardmåter å transportere disse på. Foreløpig er SAML definert bundet til SOAP over HTTP, men er tenkt utvidet til andre protokoller og underliggende kommunikasjonsmetoder. Et sentralt mål med SAML er å støtte "Single Sign-On" baserte systemer (Maler m.fl, 2003).

Ved å benytte SAML får systemet en standardisert protokoll for utveksling av autentiseringsinformasjon, som kan utvides ved fremtidige behov.

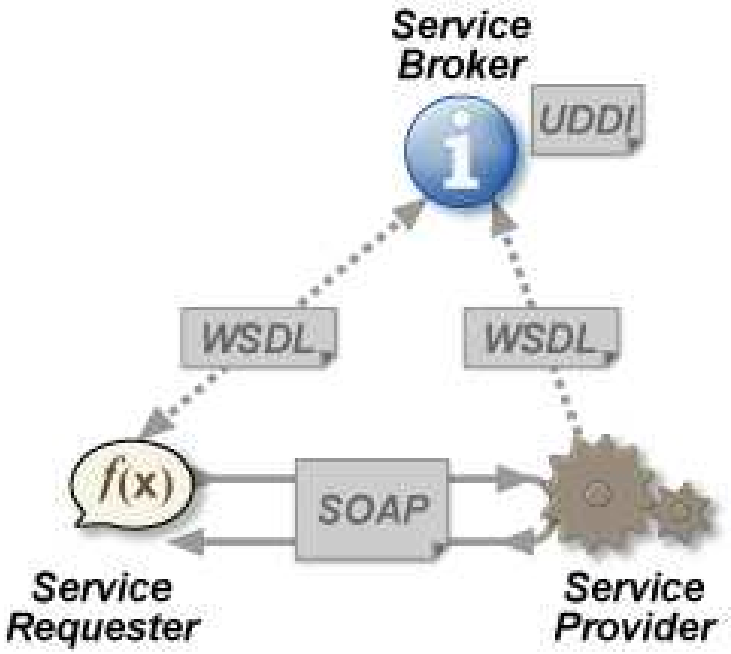
3.6.4 Web Services

En Web Service (nettjeneste) er en samling av funksjoner som er pakket i en enkel enhet og publisert på nettet for bruk av andre. Nettjenester er byggesteiner for å lage et åpent og distribuert system, og gjør det mulig for firmaer raskt og enkelt å gjøre deres tjenester tilgjengelige over hele verden (Glass, 2001). Eksempler på nettjenester

kan være kredittsjekktjenester som returnerer kredittopplysninger, oversettingstjenester som oversetter en gitt tekst fra et språk til et annet, eller værvarslingstjenester som returnerer værmeldinger for et ønsket område.

Web Services Description Language (WSDL) er et XML-format som beskriver nettjenester. Beskrivelsen inneholder tjenestens plassering og hva tjenesten inneholder. Universal Description, Discovery and Integration Service (UDDI) er en katalogtjeneste som inneholder oversikter over tilgjengelige Web Services. Kombinert gir dette muligheten til å raskt få tilgang til å benytte en lang rekke ulike tjenester som ligger tilgjengelig på nettet (UDDI.org, 2002).

Figur 3.6 illustrerer Web Services konseptet. Service Requester er ute etter en spesiell tjeneste, og henvender seg til Service Broker sin UDDI tjeneste. Der får Service Requester oversikt, og vet dermed hvilken Service Provider som tilbyr tjenesten.



Figur 3.6: Web Services illustrajon (Wikpedia.org, 2005)

MyID-konseptet er i denne oppgaven basert på én sentral Identity Provider. I et slikt tilfelle vil det ikke være nødvendig å benytte Web Services for kommunikasjon mellom IDP og SP, da SP uansett vil ha adressen til IDP liggende. Ved en eventuell utvidelse, til flere IDP'er og kan det være fordelaktig å bruke Web Services for at Service Providere enkelt skal kunne finne og kommunisere med en rekke IDP'er. Dette blir nærmere drøftet i avsnitt 8.2.

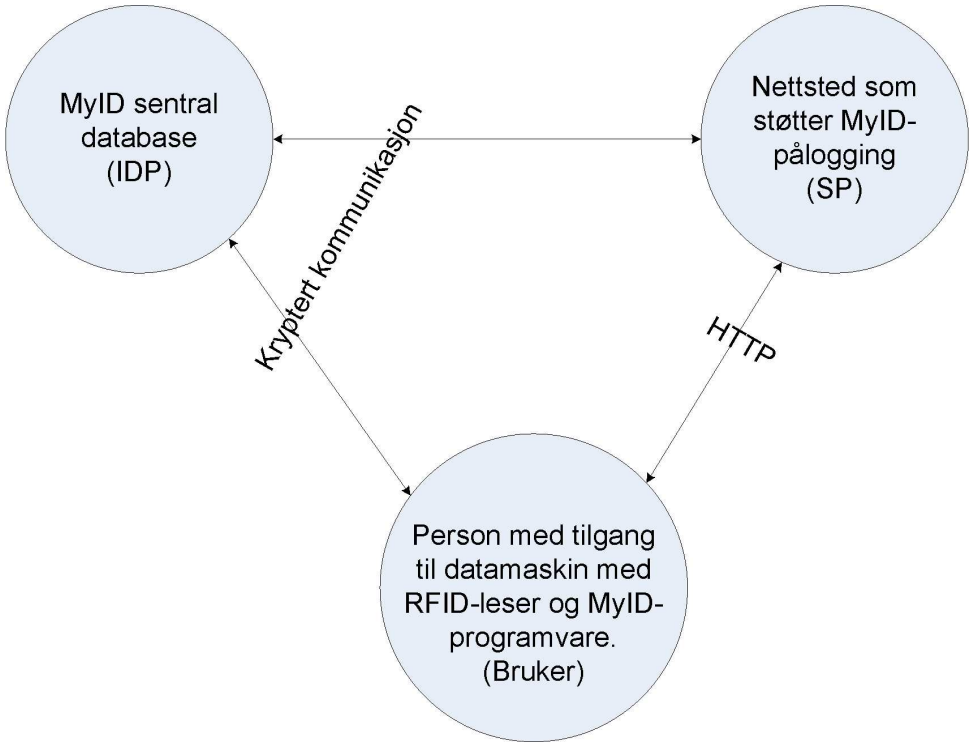
3.6.5 Kryptering

Autentiseringsinformasjon og personlige data er interessante mål for datakriminalitet. Det er derfor nødvendig å kryptere informasjonen som går mellom IDP og SP, og mel-

lom bruker og IDP. Det finnes flere måter å gjøre dette på, for eksempel ved bruk av Kerberos-protokollen. Kerberos er utviklet ved MIT (Massachusetts Institute of Technology) for å løse problemene med sikker kommunikasjon over et usikkert nettverk (MIT, 2005). Hvilken krypteringsteknologi som skal benyttes er en utfordring for videre arbeid, se avsnitt 8.2.

Kapittel 4

MyID-konseptet



Figur 4.1: Hovedaktørene i MyID-konseptet.

Kapittelet presenterer MyID-konseptet. En oversikt over de tre hovedaktørene gis i avsnitt 4.1. Avsnitt 4.2 går nærmere inn på universelle profiler og drøfter fordeler og utfordringer i forbindelse med bruk av slike. I avsnitt 4.3 drøftes den fysiske plasseringen av RFID-brikken. Figur 4.1 gir et overblikk over de tre aktørene i MyID-konseptet og kommunikasjonen mellom dem.

MyID-konseptet går ut på å eliminere dagens tungvindte autentiseringsløsninger, og erstatte disse med en RFID-basert løsning, knyttet opp mot universelle profiler og en Single Sign-on-løsning.

4.1 Aktører

Systemet har tre hovedaktører, allerede introdusert i avsnitt 1.4. Figur 4.1 viser disse i sammenheng, og de følgende avsnittene gir en nærmere beskrivelse av aktørene.

4.1.1 Bruker

Fra avsnitt 1.4 har vi at en bruker er "en person som sitter med en installasjon av MyID-systemet. Hun har en datamaskin med MyID-programvare installert, og en tilkoblet RFID-leser". Brukeren er den viktigste aktøren i konseptet, det er brukeren sine krav og ønsker som må tas hensyn til. Fremtidens kunder *vil ha det de vil ha, når de vil ha det* (Tepfers og Davidsen, 2001) , og legger på den måten premissene for hva bedriftene som ønsker å selge varer og tjenester må klare å tilby. For brukeren vil MyID-konseptet medføre mindre tid kastet bort på å registrere seg, mindre behov for å gå rundt og huske på en haug med brukernavn og passord, og en sentralisert profil som forenkler arbeidet med å holde sine personalia oppdatert.

4.1.2 Identity Provider

En Identity Provider (IDP) er i denne oppgaven en aktør med to oppgaver. For det første er det IDP sitt ansvar å autentisere brukeren, ved første innlogging overfor IDP'en selv, og deretter overfor Service Providere som henvender seg til IDP. For det andre er det hos IDP den universelle profilen (se avsnitt 4.2) ligger lagret. Identity Provider må være en frittstående aktør, gjerne finansiert i fellesskap av de Service Providere som benytter systemet, men lekkasjer av informasjon mellom IDP og SP må ikke forekomme.

4.1.3 Service Provider

En Service Provider (SP) er et nettsted som tilbyr en tjeneste til brukeren. Dette kan være nettbutikker, diskusjonsfora, flyselskaper, nettbanker og så videre. Hos SP er det beskyttede områder, som man kun får tilgang til når man er autentisert av IDP. Eksempler på dette kan være kontoinformasjon i nettbanken, mulighet for å bestille varer i nettbutikken, eller muligheten for å skrive innlegg i et diskusjonsforum. Service Provideren benytter seg av IDP for å autentisere brukeren. Fordi IDP har "godkjent" brukeren, og SP stoler på IDP, vil også SP godkjenne brukeren og gi henne tilgang til den informasjonen hun ønsker.

4.2 Universelle profiler

Autentisering ved hjelp av RFID-teknologi kan være med å eliminere behovet for en rekke brukernavn og passord, ved at brukeridentifikasjonen ligger koblet mot ID-nummeret på brikken. Likevel vil dette by på nye utfordringer, dersom hvert enkelt nettsted selv skal administrere tilleggsopplysninger slik som navn, adresse, kjøpshistorikk og så videre. Det kan derfor være hensiktsmessig å samle slike opplysninger i en sentral database, og det er her en universell profil kommer inn i bildet.

Ved å fjerne ansvaret for lagring av brukerdata og autentiseringsinformasjon fra nettstedene og samle dette i én database kan det medføre betydelige forenklinger for brukeren. Dette blir nærmere forklart i avsnitt 4.2.1, mens avsnitt 4.2.2 går nærmere inn på utfordringer knyttet til bruk av universelle profiler.

4.2.1 Forenklinger med universelle profiler

Ved å oppbevare sine personalia og preferanser i én database er det betraktelig enklere å holde denne oppdatert. En adresseendring vil typisk føre til at brukeren må logge seg inn på samtlige nettsteder hun er registrert og manuelt endre adressen. Dersom hun benytter en universell profil vil det være tilstrekkelig å endre adressen i den sentrale databasen. Nettsteder hun besøker kan istedet for å be brukeren legge inn all informasjon manuelt, hente ut data fra den universelle profilen, selvsagt kun med brukerens tillatelse. Dette kan bidra til å gjøre hverdagen enklere for den vanlige internettbruker.

Det at ymse personalia og preferanser ikke ligger lagret i noe særlig omfang på en rekke databaser rundt om kring, men istedet samles på ett sted vil gjøre det vanskeligere for ondsinnede å få tak i informasjon om brukeren. Den sentrale databasen må selvsagt være tilstrekkelig sikret.

Det eksisterer allerede enkelte slike prosjekter, som for eksempel Liberty Alliance Project. Liberty Alliance er en organisasjon opprettet for å utvikle en åpen, standardisert nett-ID for Single Sign-on (Sundsted, 2002). Det er tidligere utviklet en prototype basert på denne standarden ved IDI, NTNU (Sundsdal m.fl, 2003).

På grunn av at autentiseringen i MyID-systemet allerede foregår via en sentralisert aktør, Identity Provider, er det nærliggende å også plassere denne profilen hos IDP. Dermed blir IDP en leverandør av både autentiserings- og profiltjenesten.

Arbeids- og administrasjonsdepartementet har også et interessant system på trappene, kalt "MinSide", som skal tilby et nettsted der hver enkelt nordmann kan benytte offentlige tjenester elektronisk. Departementet ser også på mulighetene for en Single Sign-on-løsning i forbindelse med MinSide (Arbeids- og adm.dep., 2005). Konseptet virker interessant, og det kan være aktuelt å se på mulighetene for å integrere inn en mer kommersielt rettet brukerprofil i dette systemet. Dermed kan alt samles på samme sted, både offentlig rettet brukerdata og data som ønskes brukt mot kommersielle nettsteder. Isåfall vil MinSide-konseptet kunne fungere som en sentral IDP for hele Norge, og tilby hele spekteret av tjenester fra elektronisk signatur til universelle profiler.

Figur 4.2: Utdrag fra MinSide-konseptet.

Utover det rent formelle (navn, adresse, o.l), kan det lagres mye annet i en universell profil. Data som skostørrelser, preferanser for musikktype, typer mat brukeren foretrekker, og så videre kan lagres i en slik database. Dermed kan Service Providere, hvis de får tilgang til slik informasjon, personalisere de nettsidene brukeren får presentert, til å passe sammen med brukerens preferanser og ønsker. Slik personalisering i MyID-konseptet diskuteres nærmere i *Radiobrikker i handelen, K. Lilleng (2004)*, og vil derfor ikke gåes nærmere inn på her.

4.2.2 Utfordringer med universelle profiler

Misbruk av persondata er en problemstilling som blir stadig mer aktuell i et informasjonssamfunn. Hvis for eksempel et ondsinnet nettsted ønsker å misbruke de prefe-

ranser brukeren har lagret i sin personlige profil, til for eksempel å bedrive masseutsendelse av reklame, kan dette være med på å bryte ned tilliten til systemet. Det må derfor være mekanismer som minimaliserer slike potensielle problemer.

Enhver nyvinning er avhengig av tillit for å vinne frem. Å overbevise folk til å samle alle sine personlige data på ett sted kan by på store utfordringer. Det er derfor nødvendig å tilby en verdiøkning sammen med nyvinningen, slik at folk vil ønske å ta den i bruk. En Single Sign-on-løsning og autentisering basert på RFID er eksempler på en slik verdiøkning.

4.3 Plassering av brikken

Systemets portabilitet betinger at brukeren har med seg RFID-brikken overalt der hun ønsker å benytte MyID-systemet. Dermed må brikken plasseres på en gjenstand som vanligvis medbringes. Bankkort og mobiltelefon er to ting de aller fleste har med seg til daglig, og det kan derfor være aktuelt å benytte en av disse til å holde RFID-brikken. En tredje mulighet er å plassere brikken i et smykke. Dette kapittelet ser nærmere på de tre alternativene. Felles for dem er at når brukeren ønsker å benytte brikken til å logge inn på systemet må hun sørge for at den befinner seg innenfor radiusen til RFID-leseren, som oppdager brikken når den er i nærheten. Brukeren blir autentisert mot det sentrale systemet, på den aktuelle PC'en leseren er koblet til. Hun kan deretter åpne en nettside som vanligvis krever brukernavn/passord, og automatisk bli autentisert.

4.3.1 RFID på bankkortet

RFID-brikkene er såpass små at de uten problemer kan bakes inn i et vanlig bankkort. Brukeren vil dermed bære med seg sin "digitale identitet" sammen med sitt vanlige identifikasjonskort. På den måten vil samme kort bruker for betaling av varer, identifiksajon overfor andre og på nettet via MyID-konseptet. Dette er en enkel og grei løsning, som kombinert med et passord for innlogging mot Identity Provider gir en forholdsvis god sikkerhet.

Oppgaven videre baserer seg på denne plasseringen av RFID-brikken.

4.3.2 RFID i mobiltelefonen

Ved å plassere RFID-brikken i mobiltelefonen åpner det seg interessante muligheter for interaktivitet. For eksempel kan nettsteder som krever ekstra sikkerhet, typisk nettbanker, kunne be brukeren taste inn koder på telefonen før tilgang gis. Dermed vil man oppnå en ekstra sikkerhet for enkelte nettsteder. En slik plassering vil medføre at samtlige produsenter av mobiltelefoner må implementere støtte for et slikt system, noe som kan bli vanskelig å få gjennomført.

4.3.3 RFID i smykker

Et tredje alternativ kan være å plassere brikken i et slags smykke eller armbånd. Fordelen med en slik plassering er at det kan slå an som en trend, og dermed gi konseptet en rask start. På den annen side betinger det at man må gå rundt med nok en gjenstand plassert på kroppen, noe som kan få mange til å vegre seg, fordi de allerede har nok av ting å ha med seg.

4.4 Kommersialisering av konseptet

Generelt medfører innføring av et nytt system som regel kostnader, som er noe bedrifter foretrekker å holde så lave som mulig. Hvorfor skal så nettsteder og sluttbrukere investere store summer for å implementere MyID-konseptet? Avsnitt 4.4.1 ser nærmere på fordelene en bedrift kan få ved å innføre MyID, mens avsnitt 4.4.2 fokuserer på fordeler for sluttbrukeren.

4.4.1 Fordeler for Service Provider

I praksis vil ikke en Service Provider merke om brukeren benytter en RFID-basert autentisering mot Identity Provider eller ikke, så det er derfor andre fordeler disse vil være interessert i. I dag har hver eneste Service Provider vanligvis sin egen database med brukere, kunder eller lignende. Kostnadene forbundet med drifting og vedlikehold av en slik database vil forsvinne med et system som baserer seg på en sentralisert IDP hvor kundedata oppbevares. I tillegg vil man unngå problemene med degenerering av databasen, slik som utdatert og feilaktig personinformasjon.

En annen fordel en Service Provider vil ha ved å gå for MyID er at brukerne, ved at de slipper den omstendelige registreringen for å opprette en konto hos SP, lettere kan komme til å ta i bruk nettstedet. Dermed kan SP oppnå en økning i kundemassen, og samtidig unngå problemer forbundet med å vedlikeholde en voksende database.

Dersom MyID-konseptet, eller et lignende system, slår an, vil de som ikke støtter et slikt system sakke akterut og miste kunder. Ved å være tidlig ute kan Service Providere derimot nyte godt av å være blant aktørene som faktisk har implementert støtte for systemet, ved at kundene velger dem fremfor de som ikke har støtte for det.

4.4.2 Fordeler for brukerne

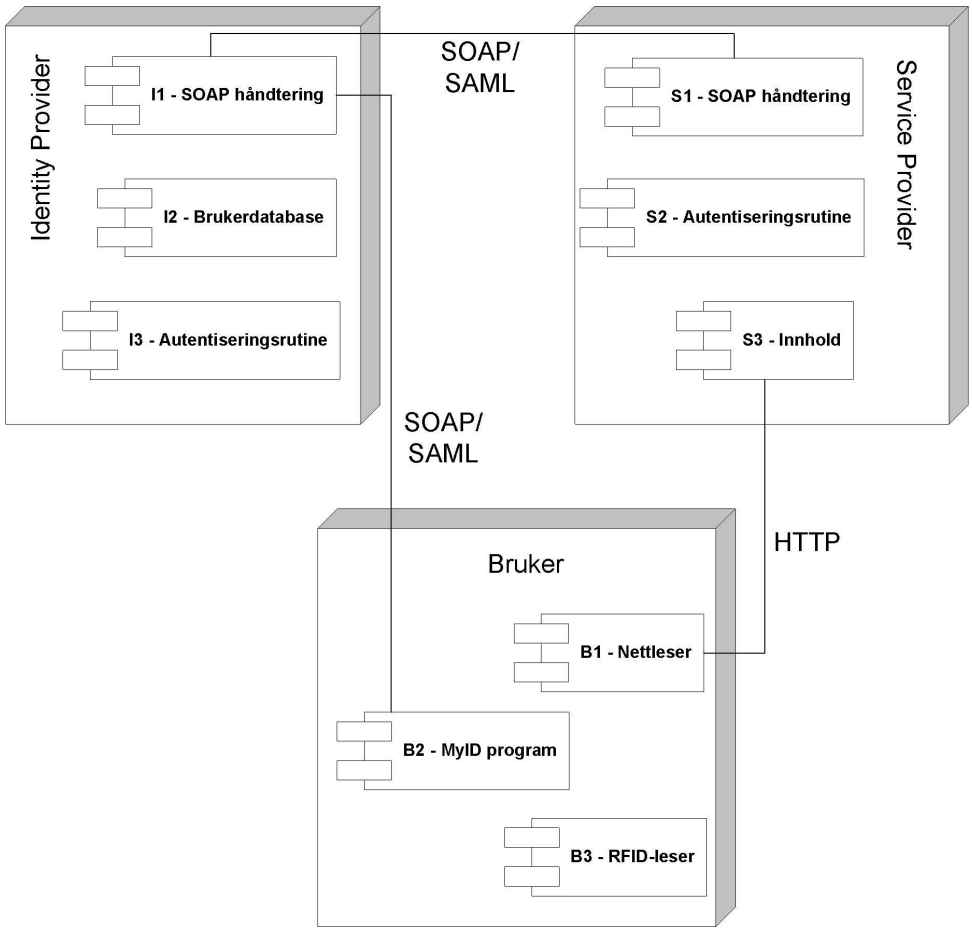
I motsetning til for Service Provideren vil det være nettopp fordelen med en RFID-basert autentisering som kan få en sluttbruker til å gå til innkjøp av en RFID-leser. I prinsippet kunne MyID vært implementert med et vanlig smartkort eller USB-nøkkel, som har en lavere pris enn en RFID-leser. Det er derimot selve trådløsheten som gjør RFID såpass attraktivt at det er valgt som grunnlag for systemet. RFID-brikken følger med brukeren sammen med bankkortet, som er noe de fleste har med seg over alt. Portabiliteten til RFID er et godt argument for å overbevise sluttbruker om å ta kostnaden med å anskaffe en RFID-leser.

Brukeren vil slippe å registrere seg på utallige nettsteder for å få tilgang til dem, noe som sparer mye tid og irritasjon med å måtte huske nok et brukernavn og passord. Kodekalkulatorer som forsvinner og smartkort som glemmes igjen hjemme vil ikke lengre være noe problem. Til slutt vil fordelen med å kun holde én database oppdatert med korrekt informasjon (hos IDP) være med på å gi brukerne en forenklet hverdag

på internett. Disse fordelene og forenklingene vil være viktige bidrag for at folk flest skal ta i bruk MyID-konseptet.

Kapittel 5

Systembeskrivelse



Figur 5.1: Overordnet arkitektur.

Kapittelet inneholder en systembeskrivelse, basert på ulike typer diagrammer og en kravspesifikasjon.

Figur 5.1 viser den overordnede arkitekturen i systemet, basert på de tre hovedaktørene som presenteres i avsnitt 4.1.

5.1 Aktørenes sammensetning

Systemets tre hovedaktører, bruker, IDP og SP, inneholder noen nødvendige komponenter som kreves for at systemet skal kunne fungere. Komponentene er illustrert i figur 5.1.

5.1.1 Bruker

Fra avsnitt 1.4 har vi at en bruker er "en person som sitter med en installasjon av MyID-systemet. Hun har en datamaskin med MyID-programvare installert, og en tilkoblet RFID-leser".

I systemsammenheng omfatter begrepet "bruker" de komponentene som må være tilstede på brukerens datamaskin.

B1 - Nettleser: Brukeren har en nettleser installert på sin datamaskin. Denne kommuniserer med Service Provider via vanlig HTTP.

B2 - MyID-program: Et program for sammenkjøring av RFID-leseren, kommunikasjon med IDP og brukerens nettleser må være installert. MyID-programmet kommuniserer med IDP ved på- og avlogging av systemet via SOAP/SAML basert kommunikasjon. Programmet gir et grensesnitt mot brukeren for å muliggjøre på- og avlogging, og vise hvilken tilstand systemet er i. Kapittel 6 illustrerer hvordan MyID-programmet ser ut for brukeren.

B3 - RFID-leser: For at MyID-kortet skal kunne avleses må det være en RFID-leser tilkoblet brukerens datamaskin. RFID-leseren oppdager og leser av MyID-kort innen rekkevidde.

5.1.2 Identity Provider

I1 - SOAP-håndtering: En komponent som tar seg av kommunikasjonen med SP. Kommunikasjonen foregår ved hjelp av SOAP og SAML.

I2 - Brukerdatabase: Personalia til alle registrerte brukere av MyID-systemet ligger lagret i brukerdatabasen.

I3 - Autentiseringsrutine: Når en bruker ønsker å logge inn på MyID-systemet er det autentiseringsrutinen som foretar kall mot brukerdatabasen og finner ut om brukeren kan autentiseres eller ikke.

5.1.3 Service Provider

S1 - SOAP-håndtering: En komponent som tar seg av kommunikasjonen med IDP. Kommunikasjonen foregår ved hjelp av SOAP og SAML.

S2 - Autentiseringsrutine: Når SP har fått klarsignal fra IDP gir den brukeren tilgang til det beskyttede innholdet. Autentiseringsrutinen hos SP sørger for å gi den rette brukeren tilgang, og for å ivareta de rutinemessige autentiseringskontrollene mot IDP.

S3 - Innhold: Beskyttet innhold hos Service Provider, som bruker får tilgang til etter at hun er autentisert. Kommunikasjon mellom Service Provider og brukerens nettleser foregår via vanlig HTTP, slik at eksisterende nettlesere kan benyttes.

5.2 Kravspesifikasjon

Kapittelet inneholder en oversikt over hvilke krav som stilles til systemet. Kravene er del inn i funksjonelle krav og ikke-funksjonelle krav.

5.2.1 Aktører

Aktørene i kravoversiktene er de samme som i 4.1, men gjentas kort her.

Aktør 1: Bruker
Beskrivelse: En person som benytter seg av MyID-systemet

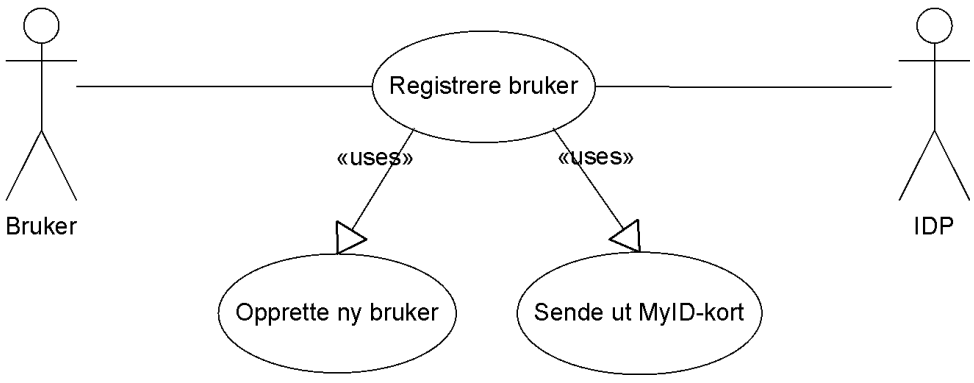
Aktør 2: Service Provider (SP)
Beskrivelse: Et nettsted som tilbyr en tjeneste.

Aktør 3: Identity Provider (IDP)
Beskrivelse: Aktøren som lagrer MyID-profilen og tilbyr autentisering.

5.2.2 Funksjonelle krav

Funksjonelle krav beskriver hva systemet skal utføre, hvordan det skal reagere og håndtere ulike situasjoner, og lignende. Kravene er illustrert ved hjelp av Use Case diagrammer.

5.2.2.1 Registrering av bruker



Figur 5.2: Use Case - Registrering av bruker

Beskrivelse
Use Case som viser hvordan brukeren blir registrert hos Identity Provider

Aktører
Bruker, IDP.

Trigger
Brukeren ønsker å ta i bruk MyID-systemet.

Standard hendelsesforløp
1. Brukeren ønsker å registrere seg.
2. IDP oppretter bruker og sender ut MyID-kort.

Alternativt hendelsesforløp
1. Brukeren ønsker å registrere seg.
2. Brukeren er allerede registrert og får beskjed om dette.

FK01: Eksistens av IDP
Det må eksistere en IDP med en brukerdatabase for at systemet skal være operativt.

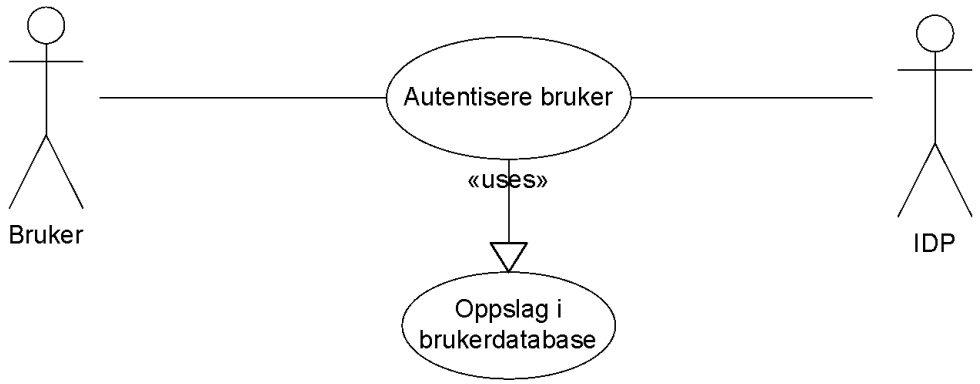
FK02: Eksistens av SP
Det må eksistere minst én SP for at det skal være noen hensikt å bruke systemet.

FK03: Registrering av bruker
Nye brukere må kunne registreres i systemet.

FK04: MyID-kort må kunne lages og sendes ut
MyID-kort må kunne lages og sendes ut. Samarbeid med utsteder av bankkort må være på plass for å få integrert RFID-brikke i kortet.

FK05: Brukeren må få beskjed om at hun er registrert
Brukeren må få uttrykkelig tilbakemelding om at hun er registrert i systemet.

5.2.2.2 Autentisering av bruker hos Identity Provider



Figur 5.3: Use Case - Autentisering av bruker

Beskrivelse
Use Case som viser hvordan brukeren blir autentisert hos Identity Provider

Aktører
Bruker, IDP.

Trigger
Brukeren ønsker å logge inn på MyID-systemet.

Standard hendelsesforløp
1. Brukeren ønsker å logge inn.
2. IDP kontrollerer autentiseringsinformasjon.
3. Brukeren blir autentisert og logget inn.

Alternativt hendelsesforløp
1. Brukeren ønsker å logge inn.
2. IDP kontrollerer autentiseringsinformasjon.
3. Brukeren blir ikke autentisert, og heller ikke logget inn.

FK06: Brukeren må ha et MyID-kort
For å benytte systemet må brukeren være i besittelse av et MyID-kort.

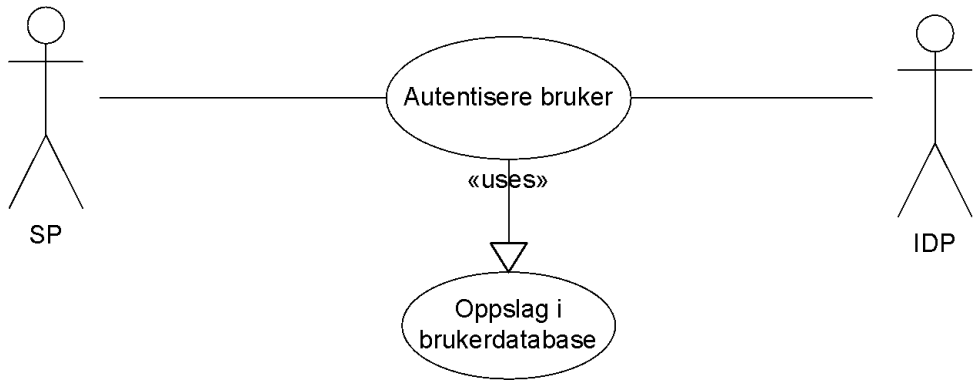
FK07: Brukeren må ha et passord
For å benytte systemet må brukeren kjenne passordet som er knyttet til sitt MyID-kort.

FK08: Eksistens av RFID-leser
En RFID-leser må være tilkoblet den aktuelle datamaskinen.

FK09: Eksistens av MyID-programvare
MyID-programvare må være installert på den aktuelle datamaskinen.

FK10: Autentisering
Systemet må være i stand til å foreta en autentisering basert på informasjon fra MyID-kortet og brukerens passord.

5.2.2.3 Autentisering av bruker hos Service Provider



Figur 5.4: Use Case - Autentisering av bruker

Beskrivelse
Use Case som viser hvordan brukeren blir autentisert hos Service Provider

Aktører
SP, IDP.

Trigger
Brukeren ønsker tilgang til et beskyttet område hos Service Provider.

Standard hendelsesforløp
1. Brukeren ønsker tilgang til beskyttet område.
2. SP foretar en autentiseringskontroll mot IDP.
3. Brukeren blir autentisert og får tilgang til ønsket informasjon.

Alternativt hendelsesforløp
1. Brukeren ønsker tilgang til beskyttet område.
2. SP foretar en autentiseringskontroll mot IDP.
3. Brukeren blir ikke autentisert og blir avvist av SP.

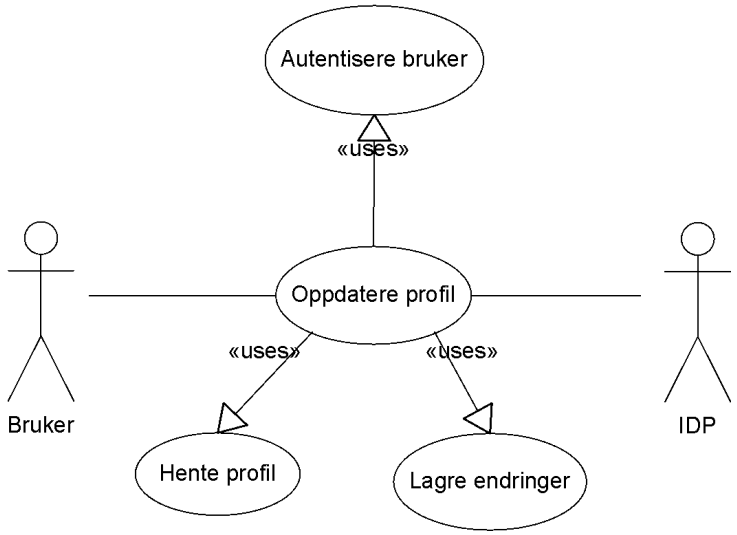
FK11: Kvalitetssikring av SP
Det må etableres en standard/godkjenningsordning for å kvalitetessikre Service Providere.

FK12: MyID-støtte hos SP
Service Provider må ha implementert støtte for MyID.

FK13: Begrenset tilgang
Service Provider må ikke ha tilgang til mer av brukerens profil enn nødvendig. Kjøpshistorikk for andre SP'ere er informasjon som ikke må deles.

FK14: Autentisering av bruker overfor SP
IDP må være i stand til å autentisere en bruker overfor en SP.

5.2.2.4 Administrasjon av profil



Figur 5.5: Use Case - Profiladministrasjon

Beskrivelse
Use Case som viser hvordan brukeren kan endre/oppdatere sin profil.

Aktører
Bruker, IDP.

Trigger
Brukeren ønsker å endre sin profil.

Standard hendelsesforløp
1. Brukeren ber om profil.
2. Brukeren får tilgang til sin profil.
3. Brukeren endrer/tilføyer/fjerner data.
4. Endringene lagres.

Alternativt hendelsesforløp
1. Brukeren ber om profil.
2. Brukeren er ikke autentisert, og får ikke tilgang til profil.

FK15: Tilgang til profil
Brukeren må ha tilgang til å se innholdet i sin profil.

FK16: Administrering av profil
Brukeren må kunne endre informasjonen som ligger lagret i profilen.

FK17: Sletting av profil
Brukeren må kunne slette sin profil og slutte å bruke MyID-systemet dersom hun ønsker det.

5.2.3 Ikke-funksjonelle krav

Ikke-funksjonelle krav legger rammene for systemet, beskriver systemets kvaliteter, og lignende.

I-FK01: Sikkerhet
Systemet må være sikkert. IDP må være tilstrekkelig sikret mot angrep og datakriminalitet.

I-FK02: Konfidensialitet
Kun autoriserte Service Providere må få tilgang til brukernes profiler.

I-FK03: Sikker kommunikasjon
Kryptert overføring mellom IDP og SP, og bruker og IDP er nødvendig for at uvedkommende ikke skal kunne snappe opp personlige data.

I-FK04: Enkelhet
Systemet må være enkelt å bruke, også for dem som har begrensete datakunnskaper. Grensensittet for administrasjon av profilen må være lettfattelig.

I-FK05: Portabilitet
Systemet må være portabelt. Det vil si at brukeren skal kunne benytte det uansett hvilken maskin hun bruker, så lenge den støtter MyID-systemet.

I-FK06: Responsibelt
Responstiden må være så god at brukeren ikke opplever irritasjon ved bruk. Tre sekunder på autentisering overfor IDP og mellom IDP og SP er absolutt maksimum tid som kan gå med til autentiseringsprosesser.

I-FK07: Tilgjengeliget
Systemet må være tilgjengelig minst 99,99% av tiden. Dette tilsvarer en nedetid på 1 time pr år.

I-FK08: Minimumsavstand
RFID-brikken må kunne avleses på minimum tre meter unna RFID-leseren.

I-FK09: Verdiøkning
Verdiøkningen for brukerne må være såpass stor at de ønsker å ta systemet i bruk. Tidsbesparing, enkel administrasjon og så videre bidrar til verdiøkning.

5.3 Systemarkitektur

Avsnittet gir en oversikt over den overordnede arkitekturen i systemet. Dataflyt- og sekvensdiagrammer beskriver hvordan systemet er ment å fungere. I dette avsnittet blir Liberty Alliance sine betegnelser IDP og SP benyttet. I dette tilfellet er IDP MyID-sentralen, mens SP er nettstedet som brukeren forsøker å få tilgang til.

5.3.1 Overordnet informasjonsflyt

Figur 5.6 viser den overordnet flyten i systemet. De tre aktørene ”Bruker”, ”IDP” og ”SP” er tatt med for å vise i hvilken rekkefølge de blir involvert i flyten. Det hele initieres av at brukerens datamaskin oppdager et MyID-kort innenfor RFID-leserens rekkevidde. Brukeren får så mulighet til å taste inn sitt passord og logge på.

Når brukeren autentiseres hos IDP genererer denne et unikt artefakt, en tekststreng, som benyttes som identifikator for brukeren resten av sesjonen. Dette artefaktet må sendes med til SP når brukeren ønsker å logge seg inn på denne ved hjelp av MyID-systemet. Artefaktet bruker SP for å kontrollere at brukeren er pålogget hos IDP og dermed autentisert for tilgang. Når SP sender artefaktet til IDP får SP tilbake en respons med hvem det er som forsøker å logge seg inn, og en bekreftelse på at denne er autentisert hos IDP. Figur 5.7 i avsnitt 5.3.2 inneholder et sekvensdiagram som illustrerer påloggingen.

HTTP-protokollen har via FORM POST funksjonen mulighet for å sende data uten at det er synlig i nettleserens adressevindu, og MyID-systemet kan benytte denne muligheten for å sende artefaktet til SP når brukeren går inn på dennes nettside.

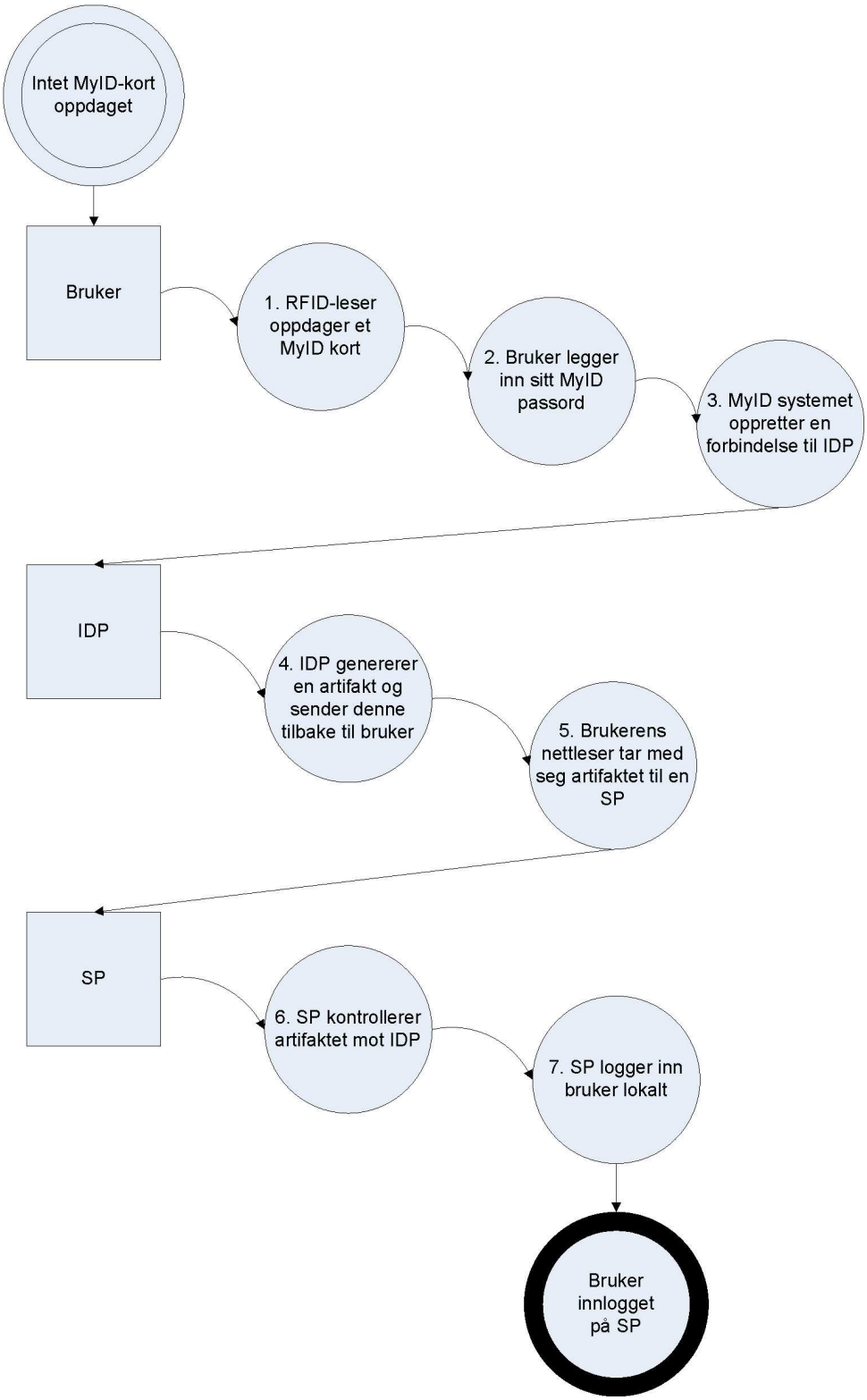
Starttilstanden er at ingen MyID-kort er oppdaget.

Bruker: Brukeren kommer innenfor RFID-leserens radius med et MyID-kort.

Steg 1: RFID-leser oppdager et MyID-kort.
Brukerens datamaskin detekterer et MyID-kort med en RFID-brikke. Systemet setter i gang og gir brukeren mulighet for å taste inn sitt MyID-passord.

Steg 2: Bruker legger inn MyID-passord.
Brukeren taster inn sitt MyID-passord og trykker på innloggingsknappen. Kortet pluss passordet er det som autentiserer brukeren overfor IDP.

Steg 3: MyID-systemet oppretter en forbindelse til IDP.
Brukerens datamaskin henvender seg til IDP via en kryptert forbindelse og sender brukerident pluss passord.



Figur 5.6: Overordnet informasjonsflyt i systemet.

IDP: IDP mottar en henvendelse fra en bruker.

Steg 4: IDP genererer en artifakt og sender denne tilbake til bruker.

IDP kontrollerer brukerident og passord mottatt, og genererer en unik artefakt som returneres til brukerens datamaskin.

Steg 5: Brukerens nettleser tar med seg artefaktet til SP.
Brukeren surfer til en SP, og med seg har nettleseren det unike artefaktet mottatt av IDP.

SP: SP mottar en henvendelse fra brukeren. Brukeren har med seg et artefakt for MyID-innlogging.

Steg 6: SP kontrollerer artefaktet mot IDP.
SP sender det mottatte artefaktet til IDP for å få informasjon om hvem det er som prøver å logge seg inn. IDP slår opp artefaktet og responderer med den tilhørende brukerinformasjonen.

Steg 7: SP logger inn bruker lokalt.
Dersom artefaktet er gyldig, og IDP svarer med brukerinformasjon, autentiserer SP brukeren og logger denne inn lokalt.

Sluttilstanden er at bruker har tilgang til det ønskede nettstedet.

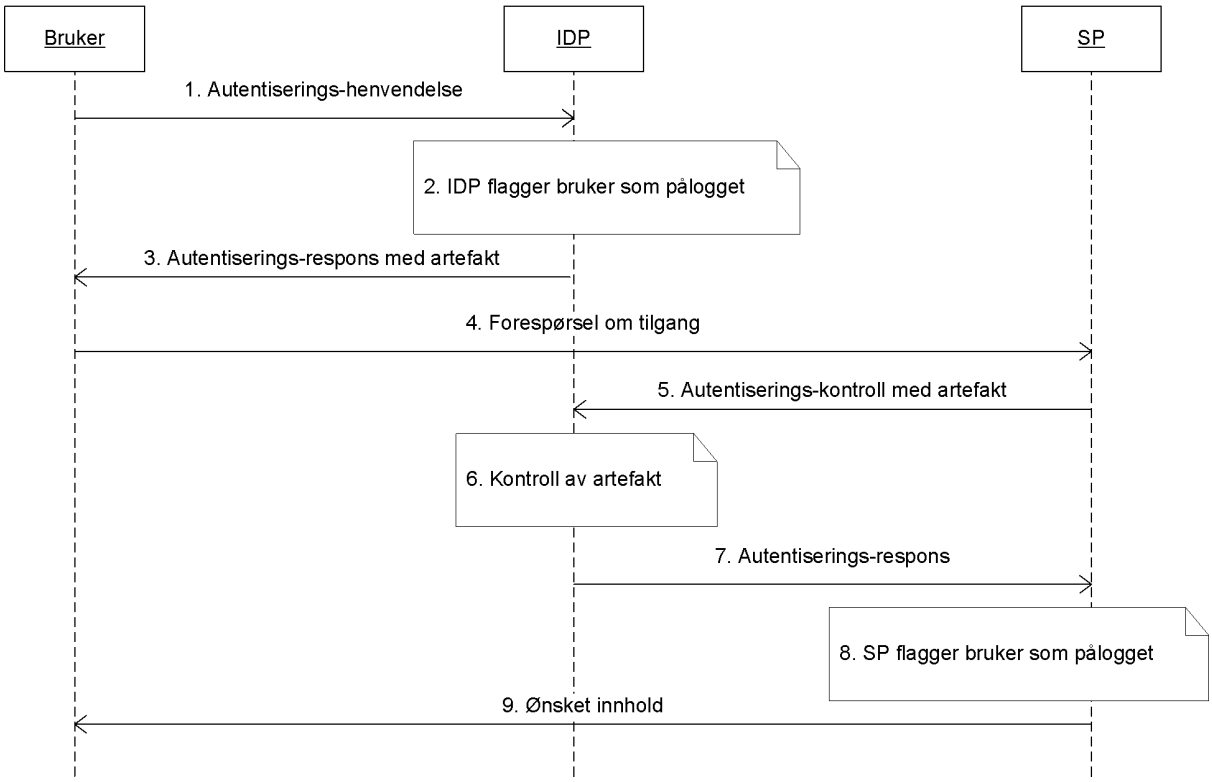
5.3.2 Pålogging

Figur 5.7 viser et sekvensdiagram som beskriver hvordan påloggingen foregår, både overfor IDP og SP. Selve autentiseringen skjer ved at IDP kontrollerer at passordet brukeren oppgir stemmer overens med brukernummeret som MyID-systemet har hentet ut fra MyID-kortet til brukeren. Senere autentisering hos SP'ere skjer ved at disse henvender seg til IDP for å kontrollere at brukeren er autentisert. Dermed behøver brukeren kun å autentisere seg én gang, og kun huske ett passord.

Steg 1: Autentiserings-henvendelse.
Brukerens datamaskin sender en henvendelse til IDP om autentisering. Henvendelsen inneholder brukerens unike brukernummer, hentet fra MyID-kortet, samt brukerens passord.

Steg 2: IDP flagger bruker som pålogget.
IDP kontrollerer at brukernummeret og passordet stemmer overens, og setter status til pålogget. IDP genererer et unikt artefakt som brukes under den aktuelle sesjonen.

Steg 3: Autentiserings-respons med artefakt.
IDP sender en bekreftelse til brukerens datamaskin på at påloggingen var vellykket. Med følger også det genererte artefaktet.



Figur 5.7: Pålogging.

Steg 4: Forespørsel om tilgang.
Bruker ønsker å få tilgang til et beskyttet område hos en SP. For eksempel en brukerkonto hos en nettbutikk. Brukerens nettleser sender med det genererte artefaktet som den mottok fra IDP.

Steg 5: Autentiserings-kontroll med artefakt.
SP sender en forespørsel til IDP for å få rede på om brukeren er logget på eller ikke. Artefaktet sendes med som identifikator.

Steg 6: Kontroll av artefakt.
IDP kontrollerer at artefaktet er gyldig, dvs om det eksisterer i en opprettet sesjon hos IDP eller ikke.

Steg 7: Autentiserings-respons.
IDP svarer på henvendelsen fra SP. Hvis artefaktet var gyldig, inneholder responsen en godkjenning for å gi tilgang.

Steg 8: SP flagger bruker som pålogget.
SP setter brukerens status som pålogget, og gir tilgang til det beskyttede området.

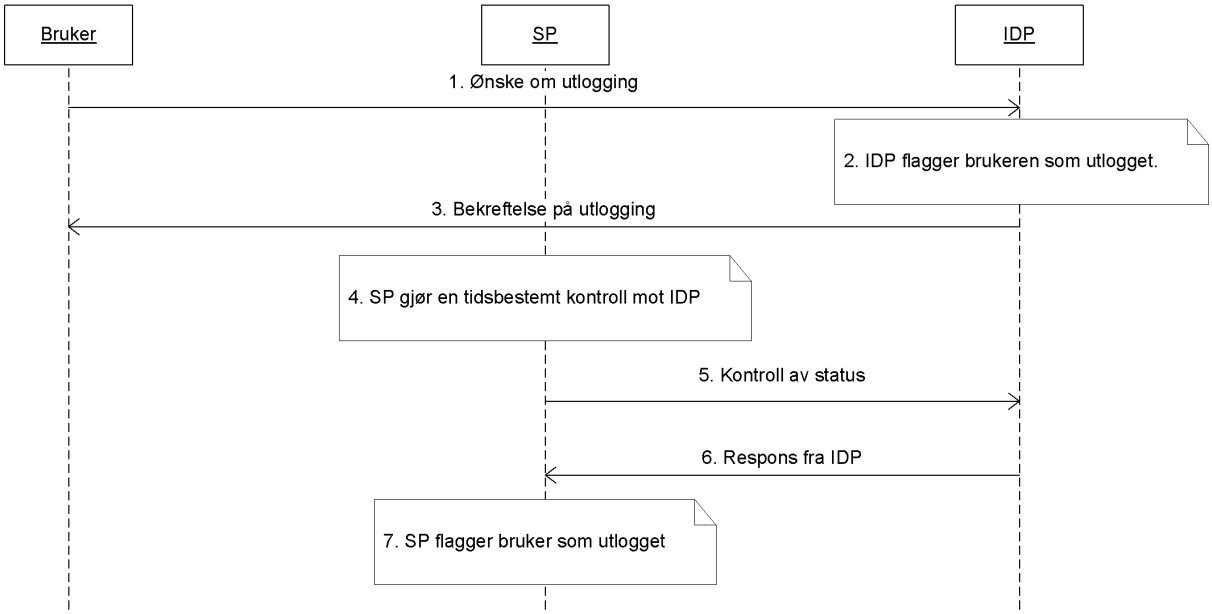
Steg 9: Ønsket innhold.
SP sender det ønskede innholdet til brukerens nettleser.

5.3.3 Global utlogging

En global utlogging foretas i det tilfelle at brukeren trykker på utloggingsknappen i MyID-kontrollpanelet. Utloggingen medfører at brukeren vil miste status som pålogget på samtlige SP'er hun er logget inn på. Når brukeren trykker på utlogginsknappen sendes en henvendelse til IDP om å sette status som ikke pålogget. Når SP gjør en tidsbesemt kontroll mot IDP for å undersøke om brukeren fortsatt er autentisert, vil den få et negativt svar. SP setter deretter status som utlogget. Hvor ofte denne tidsbestemte kontrollen skal skje er vanskelig å si, men det må ikke være så ofte at kapasiteten på nettet blir sprengt av statushenvendelser, men heller ikke så sjelden at det kan medføre noen vesentlig risiko.

Et alternativ til den tidsbestemte kontrollen er en kringkasting fra IDP til alle SP'ere som har gjort en henvendelse den aktuelle sesjonen. En slik løsning krever ekstra loggføring hos IDP, men vil til gjengjeld være mer nøyaktig enn den tidsbestemte metoden. En kringkasting kan skje umiddelbart etter at IDP har mottatt en henvendelse fra brukeren om utlogging.

Sekvensdiagrammet 5.8 illustrerer den tidsbestemte metoden for global utlogging.



Figur 5.8: Global utlogging via IDP.

Steg 1: Ønske om utlogging.
Brukeren ønsker å logge ut, og trykker på utloggingsknappen i MyID-vinduet. Systemet sender en henvendelse om dette til IDP.

Steg 2: IDP flagger bruker som utlogget.
IDP setter brukerens status til ikke pålogget, og sletter artefaktet som ble generert ved pålogging.

Steg 3: Bekreftelse på utlogging.
IDP sender en bekreftelse på utloggingen til MyID-systemet på brukerens maskin. Det endrer status til ikke lengre pålogget.

Steg 4: SP gjør en tidsbestemt kontroll mot IDP.
SP igangsetter en intervallkontroll mot IDP for å kontrollere at bruker fortsatt er pålogget.

Steg 5: Kontroll av status.
SP sender henvendelse til IDP for å kontrollere at bruker fortsatt er pålogget.

Steg 6: Respons fra IDP.
IDP svarer negativt, at brukeren er logget ut fra IDP.

Steg 7: SP flagger bruker som utlogget.
SP setter brukerens status som utlogget. Neste henvendelse fra brukeren på en beskyttet side vil medføre et avslag.

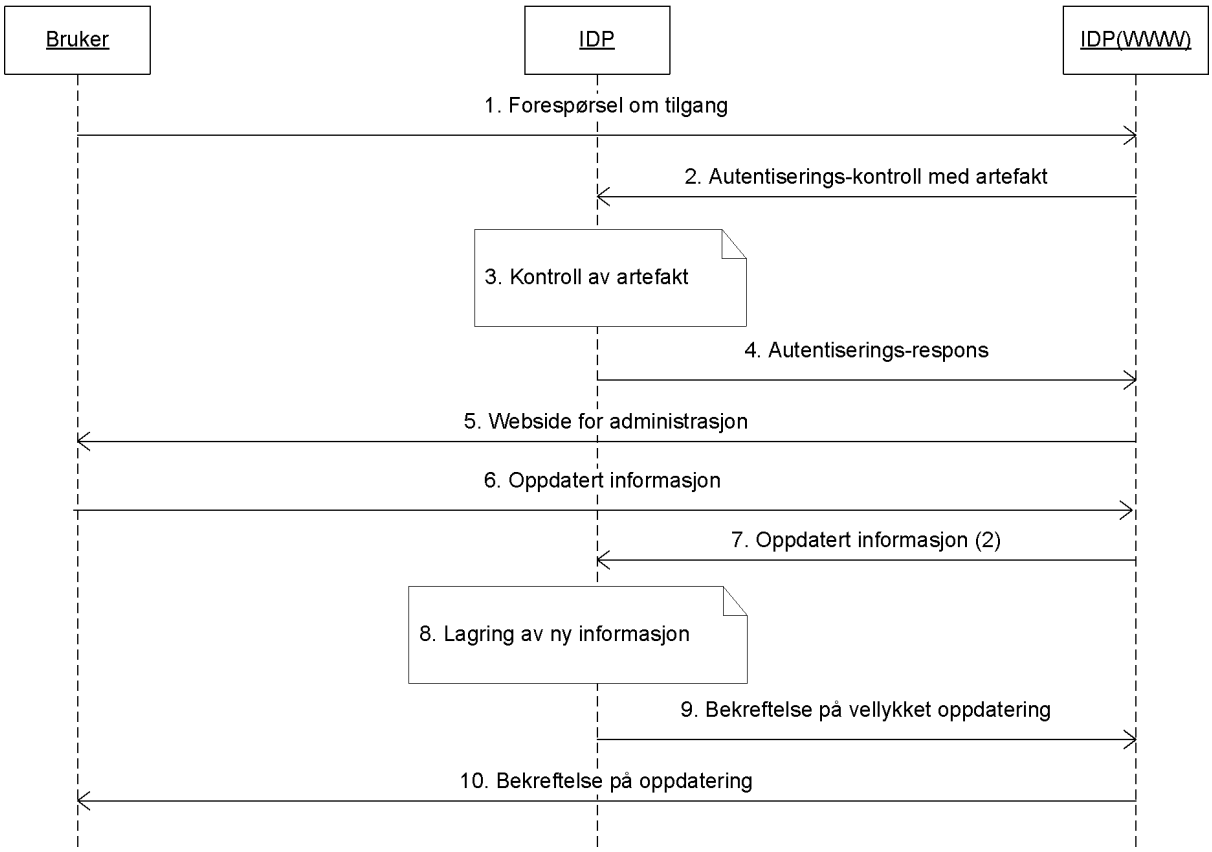
5.3.4 Administrering av profil

Dersom brukeren bytter adresse, telefonnummer eller på andre måter er nødt til å endre data lagret i profilen sin, må systemet tilby en enkel måte å oppdatere dette på. Figur 5.9 illustrerer hvordan en slik oppdatering foregår. IDP er representert to ganger i diagrammet. IDP (WWW) er i dette tilfelle det web-baserte grensesnittet som kunden møter når hun skal oppdatere profilen sin, og kan sammenlignes med en service provider. Som diagrammet viser benytter grensesnittet samme måte å kontrollere autentisering på som andre Service Providere. Diagrammet forutsetter at brukeren allerede er autentisert hos IDP.

Steg 1: Forespørsel om tilgang.
Brukeren åpner nettsiden der hun kan oppdatere profilen sin.

Steg 2: Autentiserings-kontroll med artefakt.
IDP sitt webgrensesnitt sender en forespørsel til IDP sin komponent for profilhåndtering for å få rede på om brukeren er logget på eller ikke. Artefaktet sendes med som identifikator.

Steg 3: Kontroll av artefakt.
IDP kontrollerer at artefaktet er gyldig, dvs om det eksisterer i en opprettet sesjon hos IDP eller ikke.



Figur 5.9: Oppdatering av profil.

Steg 4: Autentiserings-respons.
IDP svarer på henvendelsen fra SP. Hvis artefaktet var gyldig, inneholder responsen en godkjenning for å gi tilgang.

Steg 5: Webside for administrasjon.
Brukeren får tilgang til nettsiden der hun kan oppdatere og administrere profilen sin.

Steg 6: Oppdatert informasjon.
Brukeren sender den oppdaterte informasjonen til nettsiden (typisk ved å trykke på en ”Lagre” eller ”OK” knapp).

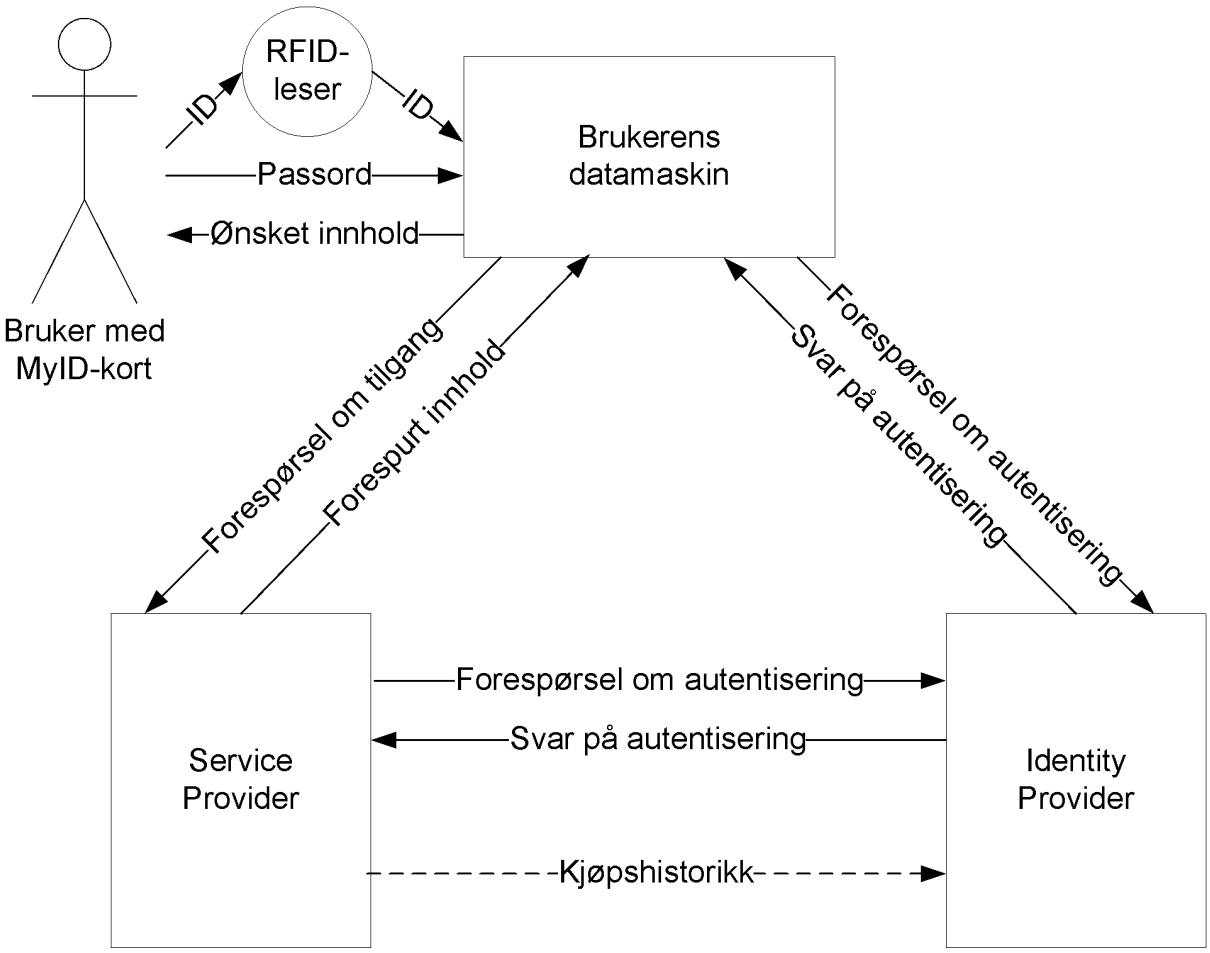
Steg 7: Oppdatert informasjon (2).
IDP's webgrensesnitt sender den oppdaterte informasjonen til profilhåndteringsdelen.

Steg 8: Lagring av ny informasjon.
IDP lagrer den oppdaterte informasjonen i sin database.

Steg 9: Bekreftelse på vellykket oppdatering.
IDP sender en bekreftelse på at oppdateringen var vellykket til webgrensesnittet.

Steg 10: Bekreftelse på oppdatering.
Brukeren mottar en bekreftelse på at oppdateringen var vellykket.

5.3.5 Overordnet dataflyt



Figur 5.10: Dataflyten i systemet.

Systemkapittelet avsluttes med figur 5.10, som viser den overordnete dataflyten i systemet. Brukeren ønsker tilgang til et beskyttet område hos Service Provider. Ved hjelp av MyID-kortet og passordet sitt, samt RFID-leseren, sendes forespørsel om autentisering til IDP. IDP svarer bekreftende. Brukeren forespør så tilgang til et beskyttet område hos Service Provider. SP sender en kontrollforespørsel til IDP, og IDP svarer bekreftende. SP sender deretter den ønskede informasjonen til brukeren.

Dersom brukeren foretar et kjøp hos SP, kan kjøpshistorikk sendes til IDP for å plasseres i brukerens profil (figur 6.6). Ved å ta i bruk profildata fra figur 6.7 i avsnitt 6.2 kan SP personalisere den informasjonen som brukeren får tilsendt. Personaliseringsaspektet ved MyID-konseptet er beskrevet nærmere i *Radiobrikker i handelen, K. Lilleng (2004)*.

Kapittel 6

Prototype

Dette kapittelet gir en visuell oversikt over hvordan systemet vil arte seg i praksis. Skjermbildene er konstruerte og demonstrerer funksjonaliteten i systemet. Avsnitt 6.1 gir et inntrykk av hvordan en innlogging med MyID fremfor brukernavn og passord kan gjøres, mens avsnitt 6.2 viser hvordan administrasjon av profilen kan foregå.

6.1 Innlogging

Figur 6.1 viser MyID kontrollpanelet. Kontrollpanelet har en hurtigknapp i oppgavelinjen: Ikonet med bokstavene ID. Bokstavene vises i blått når ingen er pålogget, og i rødt når noen er pålogget.

Figur 6.1: RFID-leseren har ikke funnet noen kort i nærheten.

Kari legger lommeboken sin med MyID kortet i nærheten av leseren og venter noen sekunder. RFID-leseren oppdager kortet og henter ut identifikasjonsnummeret og navnet som ligger lagret på det. Figur 6.2 viser dette.

Figur 6.2: Leseren har oppdaget et kort tilhørende Kari Nordmann.

Kari taster inn passordet sitt og trykker Logg inn. Systemet oppretter en sikker, kryptert forbindelse til MyID sentralen med brukernavnet (identifikasjonsnummeret) og passordet. Det stemmer over ens, og sentralen flagger Kari som pålogget. 6.3

Figur 6.3: Kari er logget inn på MyID systemet.

Kari besøker så et nettsted som krever innlogging. Innloggingsboksen fra figur 2.1 er

nå utstyrt med en egen knapp for innlogging basert på MyID. Istedet for å logge inn med brukernavn klikker hun på MyID login knappen, som vist i figur 6.4.

Figur 6.4: Kari besøker et nettsted som støtter MyID.

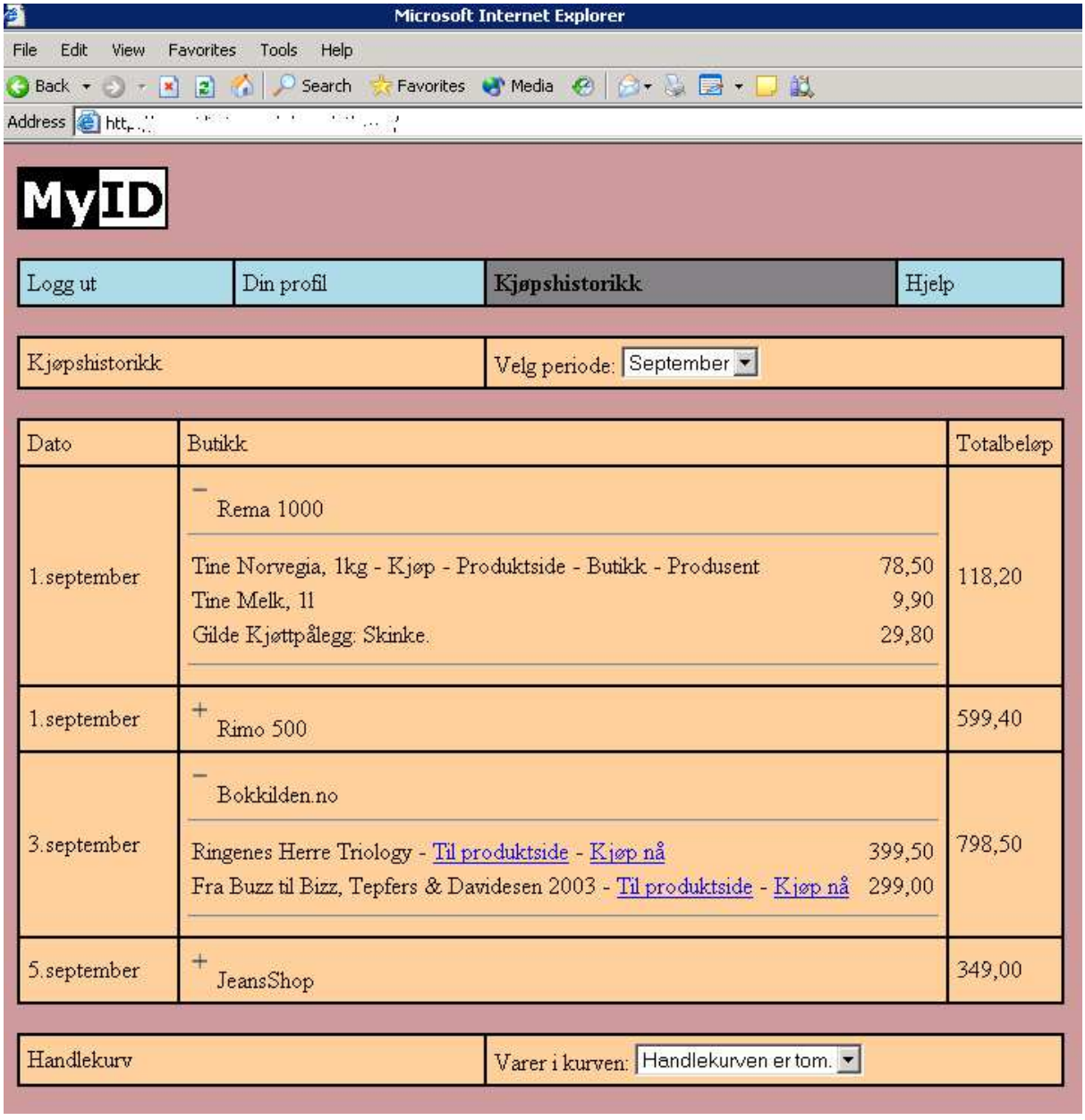
Kari blir deretter logget rett inn, på samme måte som hun ville vært ved å benytte brukernavn og passord (figur 6.5).

Figur 6.5: Kari er innlogget.

Denne prosessen kan Kari gjenta på alle Service Providere, og hun slipper å taste inn brukernavn og passord på noen av dem.

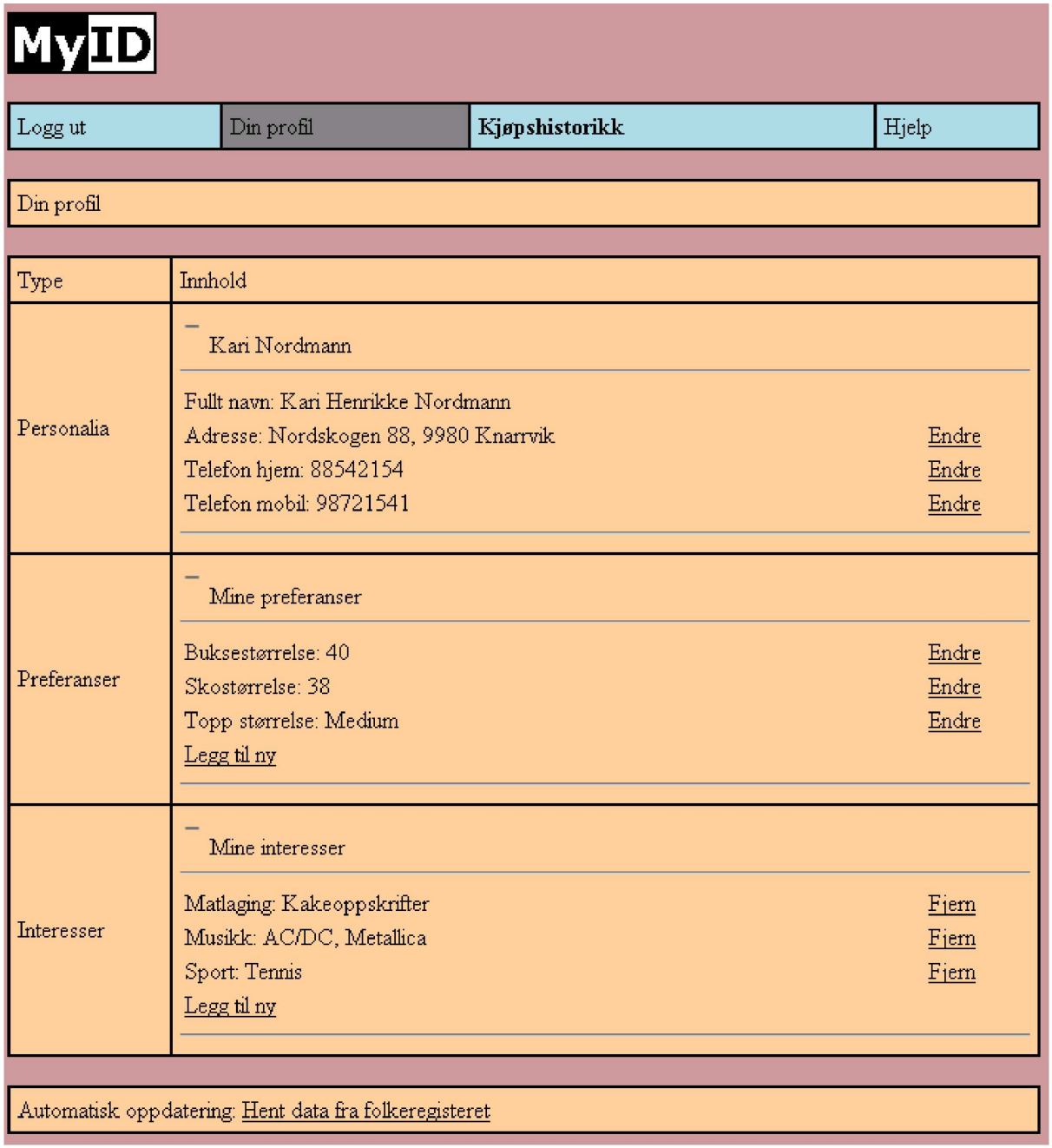
6.2 Administrasjon av profilen

Figur 6.6 er hentet fra *Radiobrikker i handelen, K. Lilleng (2004)* og viser hvordan et MyID-web-grensesnittet kan se ut. Figuren viser kjøpshistorikk og illustrerer muligheten til å kjøpe varer direkte fra MyID-grensesnittet.



Figur 6.6: Grensesnitt MyID - kjøpshistorikk.

Figur 6.7 viser hvordan MyID-grensesnittet for endring og oppdatering av den universelle profilen kan fungere. Kari har mulihet for å endre navn, adresse, interesser og preferanser. Hun har også mulighet for å hente data rett fra folkeregisteret. Dersom MinSide-konseptet fra avsnitt 4.2.1 skal benyttes sammen med MyID, kan MinSide-grensesnittet benyttes fremfor å utvikle et eget til MyID.



Figur 6.7: Grensesnitt MyID - profil.

Kapittel 7

Svakheter ved oppgaven

En betydelig svakhet med MyID-konseptet er å overbevise både kommersielle aktører og sluttbrukere om å investere betydelige beløp i å implementere et slikt system. Kostnadene vil trolig tjenes inn over tid, men inngangsprisen vil kanskje være nok til å forhindre at systemet slår igjennom. I tillegg er det ikke sikkert den trådløse fordelen er tilstrekkelig til å forsvare kostnaden: Per i dag har en vanlig smartkortleser betydelig lavere pris enn en RFID-leser.

En universell profil betinger at brukerne er villige til å dele en betydelig del personlig informasjon med en tredjepart. Det er ikke sikkert folk er interessert i dette. Det er heller ikke foretatt noen undersøkelse om hvorvidt folk faktisk vil være interessert i å ta i bruk et slikt system som oppgaven beskriver.

For at portabiliteten i systemet skal ha noen verdi er det nødvendig at flest mulig datamaskiner er utstyrt med RFID-lesere og MyID-programvare. Internettcaféer, biblioteker som tilbyr internett-tilgang, arbeidsplassen og familie og venner er alle nødt til å ta kostnadene med å kjøpe RFID-lesere. Det kan tenkes at produsentene av datamaskiner en gang vil bygge RFID-støtte inn i maskinene, noe som sannsynligvis vil kutte kostnadene betraktelig, men dette er i såfall langt frem i tid.

Systemet er heller ikke implementert i praksis, og det er ikke foretatt noen testing av hvorvidt det i det hele tatt vil fungere som denne oppgaven beskriver. Oppgaven kunne ha beskrevet arkitekturen mer detaljert for å gjøre arbeidet med en senere implementasjon enklere.

RFID-teknologien har også fått en del negativ omtale, der uttrykk som ”overvåkningssamfunn”, ”privatlivets fred” og så videre brukes flittig. Et system basert på RFID kan derfor møte sterke protester fra RFID-motstandere, og forkastet av politiske og ideologiske årsaker, selv om det viser seg å fungere i praksis.

Kapittel 8

Konklusjon og videre arbeid

8.1 Konklusjon

Etter hvert som stadig flere mennesker får tilgang til internett, og stadig flere kommersielle aktører dukker opp, vil behovet for en sikker autentisering presse seg frem. MyID-konseptet løser dette ved å tilby en trådløs, portabel autentiseringsmekanisme, kombinert med en Single Sign-on-løsning og en sentralisert universell profil.

Oppgaven har gitt en enkel innføring i RFID-teknologi, og dens fordeler og ulemper i forbindelse med MyID-konseptet. En del eksempler på dagens autentiseringsmetoder, og et scenario rundt disse, har demonstrert behovet for en ny teknologi. MyID-konseptet med universelle profiler og fordeler knyttet til bruken av slike er diskutert. En overordnet arkitektur og kravspesifikasjon er presentert, samt en prototype basert på konstruerte skjermbilder.

Oppgaven viser at en RFID-basert autentisering kombinert med en universell profil og Single Sign-on kan erstatte mange av dagens systemer for autentisering, og likevel tilby en brukervennlig, portabel og sikker løsning.

For at MyID-konseptet skal kunne lykkes på en kommersiell basis er det essensielt å kommunisere den verdiøkningen aktørene vil oppnå ved å benytte systemet. For sluttbrukeren betyr dette mindre informasjon å huske på, sentralisert administrasjon av persondata, og en portabel, trådløs brikke for autentisering. En kommersiell aktør vil kutte kostnader over tid ved å fjerne brukerdatabasen og øke inntjeningen ved at flere kunder enkelt kan ta i bruk nettstedet. Det er usikkert om disse fordelene er tilstrekkelig for å overbevise markedet, da startkostnadene tross alt er forholdsvis høye, både for sluttbrukere og kommersielle aktører. En fungerende implementasjon som kan demonstreres kan være med å hjelpe på dette.

8.2 Forslag til videre arbeid

I et videre arbeid er det en rekke ting det kan være interessant å se nærmere på. Å utarbeide en mer detaljert arkitektur, og deretter implementere systemet og starte testing av det, vil vise om det lar seg realisere i praksis i det hele tatt. Sikkerhetsaspektet bør studeres nærmere, og ulike metoder for kryptering bør undersøkes for å finne ut hvilken teknikk som egner seg best for et slikt system.

Markedsundersøkelser for å få rede på om sluttbrukere og kommersielle aktører vil være interessert i å benytte et slikt system bør foretas. Dette kan gjøres med intervjuer og demonstrasjon av en implementert testversjon. Ved å demonstrere systemet for ulike aktører vil man få en følelse for hvordan markedet vil ta i mot systemet, og om det er noe poeng i å forsøke en kommersiell lansering.

En utvidelse av systemet til flere Identity Providere kan undersøkes nærmere. Dermed kan systemet utvides til å for eksempel benyttes som trådløs identifikasjon på arbeidsplassen, som trådløst betalingskort i butikker og så videre. I så tilfelle kan det være aktuelt å ta i bruk Web Services og annen standardisert teknologi for å systematisere og standardisere kommunikasjonen i nettverket. En slik utvidelse bør ikke foretas før etter at systemet er implementert og testet med én IDP.

Tillegg A

Ordliste

Autentisering
Prosessen som gir brukeren tilgang hos en Service Provider og Identity Provider.

Brute Force
En prosess som systematisk går gjennom alle kombinasjoner til løsningen er funnet.

Identity Provider (forkortelse: IDP)
En tjener som administrerer identiteten til brukere i et MyID-system.

Nettleser
Et program som muliggjør å se på og interagere med informasjon på nettet.

Nettjeneste (eng: Web Service)
En tjeneste som tilbys på nettet. Web Service kan også i enkelte tilfeller brukes på norsk.

Transponder
Transmitter-responder. En enhet som sender et signal tilbake når den mottar et bestemt signal.

SAML
Security Assertion Markup Language. Et XML rammeverk for å utveksle autentisering- og autoriseringsinformasjon.

Service Provider (forkortelse: SP)
Her: et nettsted som støtter MyID-systemet.

Single Sign-on (forkortelse: SSO)
Egenskapen å kunne bruke beviset på en eksisterende autentiseringssesjon mot IDP, for å lage en ny autentiseringssesjon mot SP.

SOAP
Simple Object Access Protocol. En enkel mekanisme for å utveksle strukturert og typet informasjon mellom klienter i desentraliserte og distribuerte omgivelser ved å bruke XML.

Transmission Control Protocol (forkortelse: TCP)
En av kjerneprotokollene for transport av informasjon på internett.

Tjener (eng: server)
Et program som tilbyr tjenester til andre programmer på samme eller andre maskiner. Tjener brukes også om selve maskinen programmet kjører på.

World Wide Web (forkortelse: WWW)
Et informasjonsrom der ressursene identifiseres med globale identifikatorer.

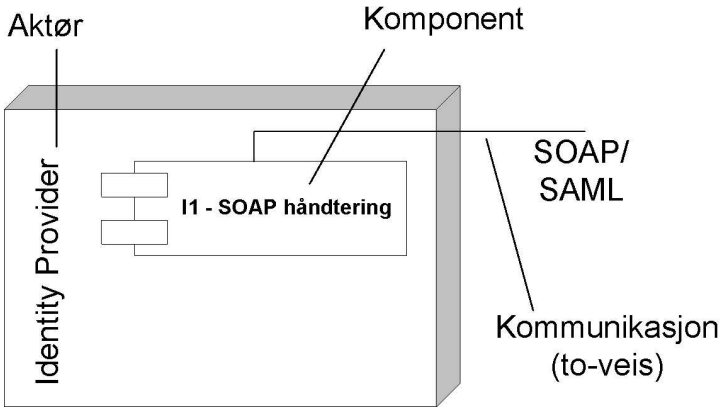
WSDL (forkortelse: WSDL)
Web Services Description Language. Et XML format som brukes for å beskrive nettjenester (Web Services).

XML (forkortelse: XML, engelsk: XML)
Extensible Markup Language. Et enkelt, men fleksibelt format for beskrivelse av informasjon. Definert av W3C.

Tillegg B

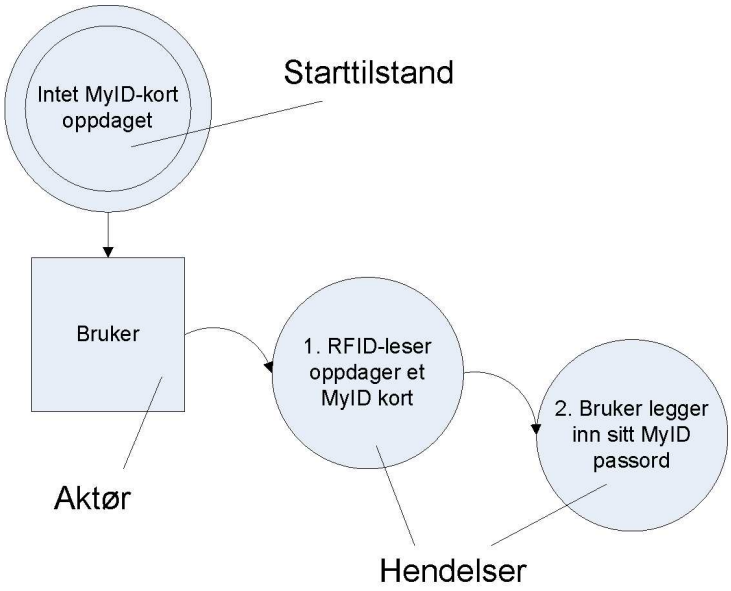
Notasjoner

UML Deployment diagram
Figur 5.1 benytter en lett modifisert utgave av UML Deployment diagram.



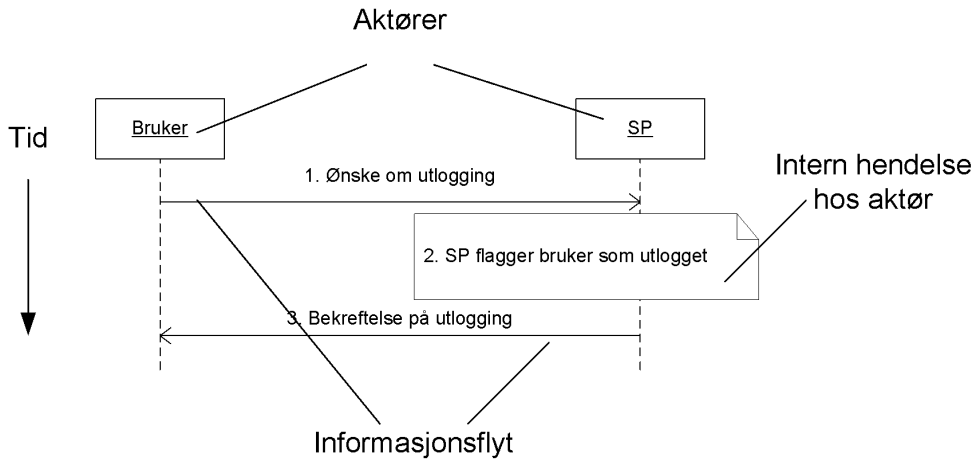
Figur B.1: Notasjon figur 5.1

Informasjonsflyt
Figur 5.6 benytter notasjon basert på DFD (Data Flow Diagram). I tillegg er de ulike aktørene tatt med, for å illustrere på hvilket tidspunkt i flyten de kommer med.



Figur B.2: Notasjon figur 5.6

UML sekvensdiagram
Notasjonen beyttet i sekvensdiagrammene er illustrert i figur B.3.



Figur B.3: Notasjon sekvensdiagrammer.

Tillegg C

Referanser

Arbeids- og administrasjonsdepartementet (2005) *MinSide testversjon*
http://www.norge.no/minside/minedata.asp

Digi.no (2002) *Hver tiende jordboer bruker Internett*
http://www.digi.no/dtno.nsf/pub/te20021119142236_qiz_53748226

Digi.no (2005) *Microsoft utvikler forbedret Passport*
http://www.digi.no/php/art.php?id=214556

Eve Maler, Prateek Mishra, and Rob Philpott (2003) *Assertions and Protocol for the Oasis Security Assertions Markup Language (SAML) v1.1*
http://www.oasis-open.org/committees/download.php/1371/oasissstc-saml-core-1.0.pdf

EPC Global (2005) *Hjemmeside*
http://www.epcglobalinc.org/

Glass,Graham (2001) *The web services (r)evolution*
http://www-106.ibm.com/developerworks/webservices/library/wspeer1.html?dwzone=ws

IAutomate.com (2005) *Home Automation RFID Reader*
http://www.iautomate.com/r500ha.html

Carbuyersnotebook.com (2005) *Exxon SpeedPass Cracked..*
http://www.carbuyersnotebook.com/archives/2005/02/exxon_speedpass.htm

Lilleng, Kaare (2005) *Radiobrikker i handelen*
Prosjektoppgave ved IDI, NTNU høsten 2004

MIT (2005) *Kerberos: The Network Authentication Protocol*
http://web.mit.edu/kerberos/www/#what_is

OpenGroup.org (Ukjent dato) *Single Sign-On*
http://www.opengroup.org/security/sso/

Procject Liberty (2005) *Liberty ID-FF Architecture Overview*
http://www.projectliberty.org/specs/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf

PSData (2005) *Hjemmeside*
http://www.psdata.no/

PSI Norge (2003) *Hva er RFID*
http://www.psi.no/produkter/rfid.htm

RFIDAsia (2003) *Rfid systems*
http://www.rfidasia.com/htmdocs/rfid systems/systems.htm

RFIDJournal (2003) *The History of RFID Technology*
http://www.rfidjournal.com/article/articleview/1338/1/129/

RFIDJournal (2004) *Alien Cuts Tag Price*
http://www.rfidjournal.com/article/articleview/857/1/1/

RFIDJournal (2004) *5-Cent Tag Unlikely in 4 Years*
http://www.rfidjournal.com/article/articleview/1098/1/1/

SpyChips.com (2004) *Images of RFID Tags*
http://www.spychips.com/tag_images.html

Statistisk Sentralbyrå (2003) *Informasjonssamfunnet*
http://www.ssb.no/emner/10/03/ikt/

Sundsdal, Fredriksen, Skuland, Sund, Stenbakk og Lilleng (2003) *Web Single Sign-on*
Kundestyrt prosjekt, IDI, NTNU høsten 2003

Symbol.com (2004) *Electronic Product Code (EPC) the RFID Standard*
http://www.symbol.com/products/whitepapers/rfid_key_issues.html#standard

Tepfers, C., Davidsen, C.M. (2001) *Konsumentkrigen*
Cappelen Akademisk Forlag.

UDDI.org (2002) *UDDI Spec Technical Committee Specification*
http://uddi.org/pubs/uddi-v3.00-published-20020719.htm

W3C (2004) *Simple Object Access Protocol (SOAP) 1.1*
http://www.w3.org/TR/SOAP

Wikipedia.org (2005) *HTTP*
http://en.wikipedia.org/wiki/Http

Wikipedia.org (2005) *Web Services*
http://en.wikipedia.org/wiki/Web_services

Wilkens, Bill (1999) *The Disadvantages of Web Cookies*
http://slis-two.lis.fsu.edu/ program/cookies/cons.html