

# **Sikkerhet i webløsninger**

## **Autentisering og tilgangskontroll**

**Versjon 1.0**

**Dato: 08.09.2003**

**KITH Rapport 30/03**

**ISBN 82-7846-194-5**

# KITH-rapport



## TITTEL

**Sikkerhet i webløsninger - Autentisering og tilgangskontroll**

Forfatter(e): Arnstein Vestad, Magnus Alsaker

Oppdragsgiver(e)

SSP

Postadresse

**Sukkerhuset  
N-7489 Trondheim**

Besøksadresse

**Sverresgt 15**

Telefon

**+47 - 73 59 86 00**

Telefaks

**+47 - 73 59 86 11**

e-post

[firmapost@kith.no](mailto:firmapost@kith.no)

Foretaksnummer

**959 925 496**

ISBN

Dato

Antall sider

Kvalitetssikret av

Gradering

82-7846-194-5

08.09.2003

24

Bjarte Aksnes

Godkjent av:  
Jacob Hygen  
Adm.dir.

Rapportnr:  
KITH R 30/03

## Sammendrag

Rapporten ser nærmere på ulike former for autentiseringsmekanismer og hvordan disse kan benyttes for å sikre webtjenester. Videre gir rapporten noen kriterier for valg av autentiseringsmekanismer. Til slutt beskrives kort noen eksempler på webtjenester som benytter ulike autentiseringsmekanismer for tilgangskontroll for kommunikasjon i helsevesenet.

# Innholdsfortegnelse

<b>Innholdsfortegnelse .....</b>	<b>3</b>
<b>1. Bakgrunn .....</b>	<b>5</b>
1.1. Lovmessige aspekter .....	6
<b>2. Autentisering, autorisering og tilgangskontroll.....</b>	<b>7</b>
2.1. Autentiseringskjeden .....	7
2.2. Identitetsbekreftelse og registrering.....	9
<b>3. Autentisering og autorisering i webtjenester.....</b>	<b>11</b>
3.1. Brukerautentisering over web.....	11
3.2. Brukersesjoner .....	12
<b>4. Kriterier for autentiseringsmekanismer .....</b>	<b>13</b>
<b>5. Autentiseringsmekanismer .....</b>	<b>15</b>
5.1. Passordbasert.....	16
5.2. Noe en har (tokens) .....	16
5.2.1. PKI .....	17
5.2.2. Smartkort .....	17
5.2.3. Software-basert.....	18
5.2.4. Mobile løsninger.....	18
5.3. Noe en er (biometriske løsninger) .....	19
<b>6. Eksempler på webløsninger.....</b>	<b>21</b>

6.1. PasientLink .....	21
6.2. medAxess.....	23
<b>Referanseliste .....</b>	<b>24</b>

# 1. Bakgrunn

Denne rapporten vil se nærmere på området autentisering og autorisering knyttet til web-tjenester. En av de fundamentale utfordringene ved elektronisk kommunikasjon innebærer å etablere tillit og sikkerhet omkring hvem man kommuniserer med. Når f.eks. enkelte aktører i helsesektoren ønsker å gi pasienter elektronisk adgang til sin egen pasientjournal er man avhengig av mekanismer som sikrer at kun pasienten selv får denne tilgangen. Når en lege oversender en elektronisk resept til et apotek må apoteket være sikker på at resepten kommer fra legen og at denne er autorisert til å skrive ut resepten. Alle disse funksjonene forutsetter sikre og tillitsvekkende mekanismer for elektronisk autentisering og autorisering.

Behovet for sikre mekanismer for autentisering og autorisering i helsesektoren er økende etter hvert som stadig nye tjenester gjøres tilgjengelig elektronisk. Det vil etter hvert være behov for mekanismer som kan autentisere både pasienter, helsepersonell og systemer overfor hverandre. Disse mekanismene vil ha varierende grad av styrke og brukervennlighet, og det vil variere hvor lett det er å integrere autentiseringsmekanismene med helsevesenets IT-systemer og applikasjoner. Denne rapporten vil se nærmere på hvilke faktorer som er av betydning ved valg av autentiseringsmekanismer og hvilke mekanismer som er egnet i ulike sammenhenger.

En mekanisme som er egnet for bruk i en sammenheng er ikke nødvendigvis egnet i andre sammenhenger. Faktorer som er særlig viktige innenfor et bruksområde kan ha mindre betydning i andre, avhengig bl.a. av risikobilde, brukernes kunnskapsnivå osv. Eksempelvis vil bruksfrekvens kunne være avgjørende for valg i enkelte sammenhenger. Hvis autentiseringsmekanismen krever at brukeren må gjennomføre en aktivitet, f.eks. taste inne en kode fra en passordkalkulator, kan mekanismen være uaktuell i sammenhenger hvor det stilles krav til raskt arbeid, hurtig tilgang til informasjon osv., som f.eks. i en behandlingssituasjon.

Denne rapporten vil stille opp noen kriterier for vurdering av autentiseringsmekanismer, slik som brukervennlighet, styrke osv., og vurdere vanlige autentiseringsmekanismer ut fra disse kriteriene. Vi vil også se nærmere på noen aktuelle implementasjoner av slike løsninger innen helsesektoren og vurdere disse.

## 1.1. Lovmessige aspekter

KITH-rapport nr. 05/2003: "Informasjonsutveksling i helsesektoren – Web-løsninger som et alternativ" går nærmere inn på bl.a. de lovmessige aspektene knyttet til utveksling av informasjon i helsesektoren, særlig knyttet opp til bruk av web-tjenester, og ser på hvilke områder web-baserte tjenester egner seg for i forbindelse med utveksling av sensitive personopplysninger.

Ut fra lovverket konkluderes det der med at ttilgang/utlevering bare kan skje såfremt det er i samsvar med gjeldende bestemmelser om taushetsplikt og personvernregler. Utlevering av opplysninger til parter utenfor den databehandlingsansvarliges virksomhet, krever en form for individuell vurdering og beslutning hos den databehandlingsansvarlige av om utlevering kan skje. Utenforståendes automatiske tilgang til opplysninger ved web-oppslag mot et sentralt nettsted (portal) for slike opplysninger uten å involvere noen person hos instansen som avgir opplysningene anses ikke tillatt. Et generelt samtykke fra pasienten på forhånd anses heller ikke å være tilstrekkelig.

Det kan likevel bl.a. tenkes løsninger hvor kun pasienten selv har web-tilgang til opplysningene og hvor pasienten kan uttrykke sitt samtykke til utlevering av opplysninger til tredjepart ved å anvende en tilstrekkelig god autentiseringsmekanisme.

Som beskrevet stilles det strenge krav til eventuelle web-løsninger som behandler sensitive personopplysninger. Denne rapporten vil ikke gå nærmere inn på de lovmessige aspektene av dette, men beskriver autentiseringsmekansimer og teknikker som kan benyttes for å gi tilstrekkelig sikkerhet ift. autentiseringen i eventuelle systemer som utvikles.

## 2. Autentisering, autorisering og tilgangskontroll

Autentisering betegner normalt en prosess hvor en bruker identifiserer seg for et system eller beviser sine rettigheter til å benytte en identitet i et system. Tidligere har dette som oftest foregått ved at brukeren oppgir et brukernavn (sin identitet i systemet) og et passord for å bevise sin rett til brukernavnet. Som oftest er formålet å få tilgang til informasjon som er begrenset til personens bruker (f.eks. e-post), og for å kunne spore endringer tilbake til brukeren.

Tilgangskontroll følger logisk etter autentisering. Når brukeridentiteten er etablert er mulig å avgjøre hvorvidt brukeren kan aksessere en gitt ressurs, f.eks. lese en fil. Med mindre man har en sikker autentisering kan ikke systemet skille mellom autoriserte og ikke-autorisert tilgang og bruk.

Autorisering kommer inn mellom autentisering og tilgangskontroll og betegner prosessen med å gi en bruker tilgang til å gjøre noe i systemet, som å lese, skrive, slette osv.

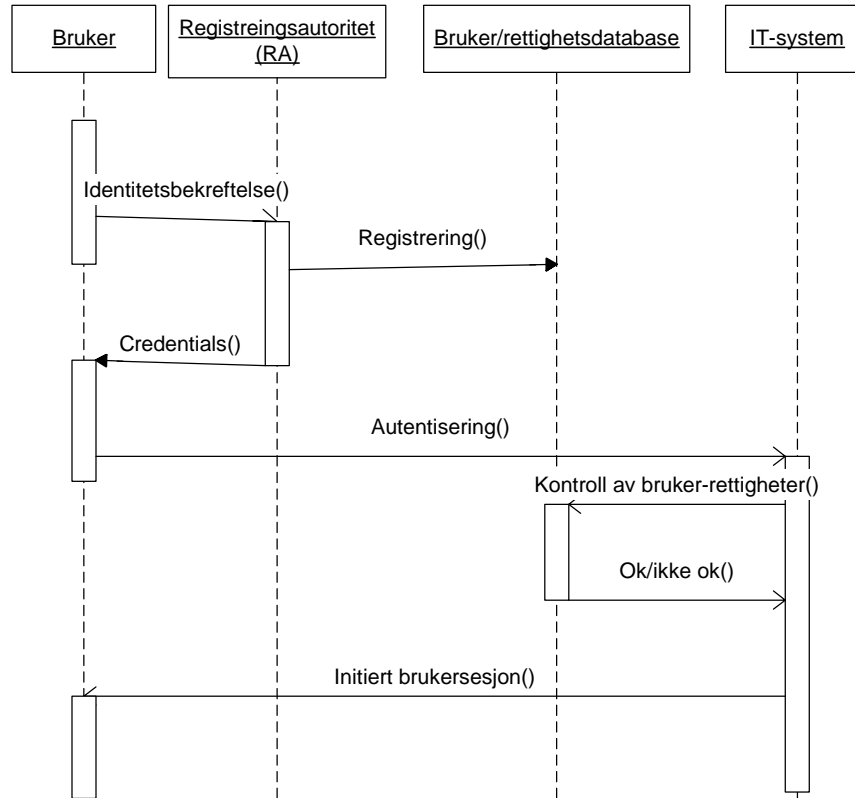
### 2.1. Autentiseringskjeden

Før brukeren i det hele tatt kan autentisere seg mot et IT-system må det være foretatt en sekvens av hendelser med formål å etablere brukeridentiteten i IT-systemet og å knytte denne opp mot brukerens faktiske identitet. Denne prosessen utgjør fundamentet for autentiseringen og feil og svakheter i denne prosessen gjør senere autentisering verdiløs.

Autentisering og identitetsbekreftelse kan ses på som en kjede med formålet å knytte en brukerkonto/brukerid i systemet til en identitet i den fysiske verden.

Grovt sett kan vi dele autentiseringskjeden inn i følgende ledd:

1. **Identitetsbekreftelse** – Brukeren må bekrefte sin identitet, f.eks. ved å vise identitetspapirer, pass, førerkort, eller ved å oppgi informasjon om seg selv, f.eks. adresse eller telefonnr, eller ved at brukeren er kjent fra før.



2. **Registrering** – Informasjon om brukeren, dvs. ulike attributter/egenskaper som det er ønskelig å knytte til brukeridentiteten registreres. Dette kan også innebære tildeling av rettigheter i systemet, f.eks. lese og skrivetilgang.
3. **Generering** – ”Credentials” – Det brukeren skal benytte for å autentisere seg overfor systemet genereres, dette kan være passord som utstedes eller velges, smartkort som initialiseres, software-token som genereres.
4. **Overføring** – ”Credentials” overføres til brukeren, dette kan innebære å informere brukeren om passordet, sende et smartkort i posten osv.
5. **Autentisering** – Når brukeren skal knytte seg til den elektroniske tjenesten benytter han sine ”Credentials” til å bekrefte sin identitet og knytte denne til en brukerid i systemet.
6. **Sesjongsenerering** – Systemet initierer en sesjon som lar brukeren benytte tjenestene som tilbys basert på de rettigheter brukeren har. Sesjonen kan initieres med et sett av rettigheter

knyttet til brukeridentiteten som igjen kan brukes til å styre tilgangen til informasjon i systemet.

En kjede er ikke sterkere enn sitt svakeste ledd, og alle leddene som er beskrevet ovenfor må derfor ha en tilstrekkelig grad av sikkerhet ift. bruksområdet, noe som innebærer en risikovurdering. For hvert ledd blir det vesentlig å vurdere hvor lett det er å misbruke svakheter i prosessen, det være seg dårlige prosedyrer for kontroll av legitimasjon eller svake algoritmer for generering av sesjonsidentitet.

## 2.2. Identitetsbekreftelse og registrering

Det første trinnet i prosessen med å etablere en tiltrodd elektronisk identitet er å bekrefte identiteten overfor noen som er autorisert til å opprette den elektroniske identiteten.

Vi kan skille mellom tre hovedstrategier for identitetsbekreftelse og brukergenerering:

1. Anonyme brukerkontoer – Det foregår ingen kontroll av offisiell identitet ved opprettelse av brukerkontoen.
2. Selvstendig kontroll av offisiell identitet.
3. Tiltrodd tredjepart håndterer kontroll av offisiell identitet.

I det første tilfellet ser man bort fra behovet for sporbarhet, dvs. muligheten for å knytte handlinger utført i systemet opp mot en konkret person (sporbarhet til brukerkonto eksisterer, men det siste leddet i kjeden mangler). Slike løsninger har både fordeler og ulemper i ulike sammenhenger. Muligheten for å opptre med en grad av anonymitet kan vise seg nyttig bl.a. i behandlingen av psykiske lidelser. Anonymiteten kan gjøre det lettere for pasienter å vise åpenhet i behandlingssituasjonen og kan også gjøre det lettere å ta kontakt med helsevesenet.

Anonymiteten kan også ha uheldige sider, bl.a. ved at helsepersonellet mangler muligheten til å ta kontakt med brukeren, f.eks. for å avverge kritiske situasjoner. Slike utfordringer skaper etiske problemstillinger som bør vurderes nærmere ved iverksetting av denne type prosjekter.

Graden av identitetskontroll i enkelte løsninger fører også med seg en grad av ”ufrivillig” anonymitet. F.eks. utføres det i en del internett-baserte løsninger for autentisering som bl.a. Microsoft Passport, liten grad av kontroll med identiteten, og det er åpent for en bruker f.eks. å opprette flere uavhengige brukeridentiteter. Slike løsninger vil derfor være lite egnet for bl.a. tilgang til pasientopplysninger osv.

I de fleste sammenhenger håndterer en organisasjon sine brukere på egenhånd. Dette gjøres på ulike måter, i større virksomheter prioriteres ofte å bygge opp et enhetlig system for brukerhåndtering med en felles brukerdatabase. Denne databasen kan så brukes for autentisering og tilgangskontroll i alle systemene i organisasjonen, det være Windows-dokumenter, UNIX-servere, EPJ og PACS-systemer. En forutsetning for at dette kan fungere er at de ulike delsystemene støtter den felles brukerdatabase f.eks. gjennom et felles grensesnitt som LDAP. Slike løsninger kan utvikles til å bli fleksible og kraftige verktøy for brukerhåndtering og kan utvides videre f.eks. til å styre installasjon og tilgang til applikasjoner på den enkelte PC.

En større utfordring oppstår når behovet for kommunikasjon på tvers av organisatoriske grenser oppstår. I og med at den ene virksomheten ikke uten videre stoler på brukerinformasjon fra den andre virksomheten er det nødvendig å finne en felles løsning med tillit fra alle partene involvert. En slik organisering baserer seg normalt på såkalte tiltrodde tredjeparter (TTP'er). TTP'en tjener som en uavhengig part som skal ha tillit fra alle partene som kommuniserer. Denne tilliten kan bygges på ulike måter, og lovverk og offentlig regulering kan være aktuelle. I Norge er TTP'er for sertifikater som skal benyttes til såkalte kvalifiserte elektroniske signaturer regulert gjennom lov om elektroniske signaturer. Dette innebærer en offentlig regulering av de prosedyrer TTP'en arbeider etter, bla. krav til fysisk sikkerhet, informasjonssikkerhet, kontroll med egne ansatte og med prosessen for å utstede sertifikater.

## 3. Autentisering og autorisering i webtjenester

Ved bruk av autentisering i web-tjenester er det viktig å skille mellom to hovedtyper autentisering, brukerautentisering og sesjonsautentisering. I en typisk brukssituasjon autentiseres normalt brukeren først ved bruk av passord, sertifikat e.l., hvorpå web-serveren genererer en sesjonsidentifikator som gis til brukerens web-leser (i en "cookie"). På denne måten kan web-leseren sende over denne identifikatoren hver gang den henter en side fra serveren og dermed autentisere seg selv. Mens brukerautentiseringen normalt foregår en gang per sesjon, foregår altså sesjonsautentiseringen hver gang web-leseren kobler seg opp mot serveren.

### 3.1. Brukerautentisering over web

Det er ulike måter å gjøre brukerautentisering over web, og autentiseringen kan gjøres vha. mekanismer innebygd i http-protokollen eller i applikasjonene bygd over protokollen.

HTTP BASIC er den enkleste formen for autentisering innebygd i http-protokollen. Når brukerens webleser ber web-serveren om en ressurs, returnerer serveren feilkoden "http/1.1 401 Authorization Required". Webleseren vil da normalt spørre brukeren om brukernavn/passord, som så overføres. Brukernavn og passord overføres i klartekst og overføringen må derfor sikres med SSL eller TLS.

HTTP DIGEST ble utviklet for å hindre at brukernavn/passord ble overført i klartekst. Autentiseringen iverksettes på samme måte som for basic, men serveren ber i tillegg om digest-autentisering. Brukeren genererer så en hash-verdi av passordet/brukernavnet, samt en tilfeldig verdi.

I stedet for å benytte seg av autentisering innebygd i http-protokollen kan utviklere av Web-applikasjoner velge å legge inn autentisering i selve applikasjonen. Dette har vanligvis blitt gjort med html-forms for å spørre om brukernavn og passord, og html-forms støtter input-typen PASSWORD som sørger for at passord framstår på formen "\*\*\*\*\*" på skjermen. Ved bruk av denne typen autentisering er det viktig at siden overføres vha. POST og ikke GET, da den siste kan medføre at forespørselen inkl. brukerens brukernavn/passord vises i URL og lagres i browserens history. Utvikleren av slike løsninger må også ta høyde for de typer angrep som http digest ble utviklet for å

beskytte mot, som at passord overføres i klartekst, at autentiseringsinformasjonen kan kopieres og sendes på nytt for å autentisere mot samme ressurs (replay attack) osv.

I tillegg til bruk av brukernavn/passord kan weblesere vha. SSL/TLS også støtte bruken av digitale sertifikater for autentisering. Sertifikatene kan lagres kryptert på harddisk eller på smartkort og kan gi en ekstra sikkerhet ift. kun brukernavn/passord.

## 3.2. Brukersesjoner

http er i utgangspunktet en "tilstandsløs" protokoll, dvs. at web-serveren bl.a. ikke husker en bruker mellom hver gang brukeren laster ned en side. Dette gjør at web-serveren bl.a. i utgangspunktet ikke kan huske en bruker og bygge opp en sesjon med denne brukeren, funksjonalitet som er blitt stadig mer utbredt bl.a. i handlekurver, for å gi tilgang til e-post osv. Problemet løses vha. "cookies", informasjonsenheter som lagres i brukerens web-leser og som web-leseren sender til serveren ved hver forespørsel. Denne "cookie" en kan inneholde en unik bruker-id som lar en web-applikasjon identifisere brukeren mellom hver forespørsel.

Når "cookies" skal brukes for å håndtere brukersesjoner er det flere faktorer som må ivaretas for å få en sikker løsning. Sesjonsid-ene må være unike og uforutsigbare og fortrinnsvis være knyttet til én klient-instans for å motvirke sesjonskaping (at noen tar over sesjonen vha. id'en) og repetisjonsangrep (at id'en benyttes på nytt). Id'en må ha tilstrekkelig nøkkel-rom til å hindre en angriper til å prøve alle mulige sesjons'ider. I tillegg kan systemet støtte utstenging av klienter som prøver ut flere sesjonsid-er.

Sesjonshåndteringssystemet bør ha en "time-out"-funksjon som gjør at en sesjon som er inaktiv over lengre tid ikke kan gjenopptas. F.eks. kan systemet logge ut en bruker som ikke har vært aktiv de siste 5-10 minuttene og kreve at brukeren autentiserer seg på nytt.

## 4. Kriterier for autentiseringsmekanismer

Etter å ha gjennomført en trusselvurdering for applikasjonen og vurdert svakheter og sårbarheter kan denne informasjonen benyttes til å stille krav til autentiseringsmekanismen. Ved evaluering av ulike alternativer er det en rekke ulike informasjonskilder som kan benyttes, f.eks. produktbrosjyrer, resultater av sikkerhetsevalueringer, forbrukertester, artikler fra IT-sikkerhetskonferanser osv. Som minimum bør de følgende kriteriene vurderes:

1. Styrke/nøyaktighet – fare for misbruk/kopiering: Autentiseringsmekanismen må ha en styrke som gjør at den med en tilstrekkelig grad av sikkerhet kan knytte en gitt person til brukeridentiteten. Den må ikke uten videre kunne kopieres slik at flere kan benytte samme autentiseringsmekanisme samtidig. Styrken i mekanismen kan f.eks. avhenge av kompleksiteten i de underliggende algoritmene som mekanismen benytter, f.eks. hvor mange tegn det er i et passord eller hvor mange bits det er i en krypteringsnøkkel.
2. Gjennomførbarhet/implementerbarhet – Mekanismene kan variere i hvor lett de lar seg implementere. Strengt krav til legitimasjonskontroll, krav til at brukeren skal inneha spesielt utstyr som smartkortlesere osv. kan gjøre systemet vanskelig å innføre.
3. Brukervennlighet inkl. ”brukerbelastning”, portabilitet/mobilitet, mulighet for å miste/ødelegge, behov for ekstrautstyr. Raskt, lett å bruke.
4. Kostnad, (f.eks. pr. gang (mobil), anskaffelse) – Kostnadene ved systemet kan deles inn i implementasjonskostnader og driftskostnader, og kostnadene kan også fordeles forskjellig mellom brukerne og den som krever autentisering. F.eks. kan en løsning som krever kostnader ift. telekommunikasjon ved hver bruk få større driftskostnader, mens en løsning som krever mye investering i utstyr før systemet settes i bruk vil få større initielle kostnader som kan skremme bort brukere hvis disse må betale alle kostnadene ved løsningen.
5. Pålitelighet – Brukerne må kunne stole på at systemet er tilgjengelig og fungerer kontinuerlig. En sentralisert løsning for autentisering, f.eks. en løsning som avhenger av kontroll av sperrelistes, vil ha større krav til tilgjengelighet, særlig hvis løsningen benyttes for å autentisere mot en rekke ulike tjenester, enn det en enklere løsning f.eks. hvor autentiseringen er innebygd i den enkelte applikasjonen har. Gjennomsnittelig tilgjengelighet kan være en viktig faktor å

vurdere ved en risikovurdering, siden manglende autentisering vil medføre at systemet er utilgjengelig for brukeren.

6. Kommersiell tilgjengelighet – Er løsningen kommersielt tilgjengelig, benyttes den av flere aktører som har implementert løsningen i sine systemer? Dette kan ha betydning for tilliten brukeren vil ha til løsningen, samt hvorvidt support, oppgraderinger osv. vil være tilgjengelig f.eks. hvis det avdekkes svakheter i løsningen.
7. Interoperabilitet, gjenbrukbarhet – Kan løsningen benyttes i flere sammenhenger, f.eks. for autentisering mot ulike systemer og tjenester, også tjenester levert av andre leverandører. Dette kan være en faktor som bidrar til å skape brukeraksept for løsningen.
8. Helhets-tillit (f.eks. til registrering) - I hvilken grad føler de som vil være avhengig av løsningen seg trygg på at løsningen tilfredsstiller deres behov. Tillit kan være vanskelig å måle konkret, men påvirkes f.eks. av dårlig mediedekning av et produkt, historie av avdekkede svakheter osv.

## 5. Autentiseringsmekanismer

Autentisering blir stadig viktigere for datasikkerheten i dagens IT-systemer. Den fysiske hindringen ved at PC-er med IT-systemer kun var tilgjengelige der de var plassert i en bygning finnes ofte ikke lenger. Utviklingen av flerbrukersystemer og systemer tilgjengelige via Internett har gjort at brukere kan autentisere seg og få tilgang til systemet nesten fra hvor som helst. Dette har ført til at autentiseringen av brukere stiller høyere krav til sikkerhet en før.

Det er tre hovedfaktorer som kan brukes gjennom autentiseringsmetoder:

1. **Noe en vet** - for eksempel brukernavn og passord
2. **Noe en er i besittelse av** (også kalt "token") - for eksempel et smartkort
3. **Noe en er** - for eksempel fingeravtrykk

I tillegg kan også følgende "metoder" brukes i en autentiseringsprosess:

4. Identiteten (den som skal autentiseres) er på en spesiell plass (til en spesiell tid)
5. Autentiseringen er etablert av en tredjepart

Det fjerde punktet er utelukket å benytte når det er snakk om autentisering på et websystem, men kan benyttes hos andre former for systemer som krever autentisering. Det femte punktet kan kombineres med "noe en er i besittelse av" slik at for eksempel det benyttes digitale sertifikater som er utstedt av en "godkjent" tredjepart.

Et system som har høye krav til sikkerhet kan benytte seg av flere av de ulike autentiseringsmetodene (eksempelvis bruk av et smartkort i tillegg til brukernavn og passord).

Dersom en benytter seg av noe som brukeren vet i tillegg til noe som brukeren har sier en ofte at det foregår en "to-faktor" autentisering fordi en bruker to ulike faktorer i autentiseringsprosessen.

Det beskrives her metoder utelukkende til bruk for identitetsautentisering (dvs. autentisering av personer, organisasjoner, virksomheter eller lignende). Autentisering av data vil ikke beskrives her (for eksempel autentisering av datainnhold og dataopprinnelse).

## 5.1. Passordbasert

Brukernavn og passord er den mest vanlige formen for autentisering som benyttes på IT-systemer. Hovedfordelen med passordbasert autentisering er at det er lett å implementere løsningen og den krever kun software. Bruk av passord har likevel flere potensielle svakheter og problemer som gjør at det ofte er lite egnet i sammenhenger med høye krav til sikkerhet. Brukernavn/passord kan også benyttes som første fase i en autentiseringsprosess hvor det stilles høye krav til sikkerheten. Brukernavn/passord blir nærmest da ”vis meg hvem du er”, mens andre fasen i autentiseringen blir ”bevis at du er den du påstår du er” (for eksempel med bruk av smart kort, digitale sertifikater eller andre ting).

Trusler mot systemer som kun benytter passord er:

- Kan være lett å avsløre (skrevet ned passord på lapp under tastaturet)
- Kan være lett å gjette (passordet er navn på familiemedlemmer, fødselsmåned, bilmerke eller lignende)
- Er lett å ”snappe” opp fordi de ofte sendes i klartekst over kommunikasjonslinjer
- Blir sjelden endret

Engangspassord blir benyttet i en del løsninger som andre fase av autentiseringsprosessen.

Engangspassord vil i praksis si at det på en eller annen måte genereres et nytt passord hver gang en autentisering skal skje. Engangspassord kan kun benyttes i en bestemt autentiseringsprosess og det kan ikke brukes i senere autentiseringer. Passordgeneratorer bør være utformet slik at det ikke er mulig å finne ut det neste passordet selv om en vet de foregående. Dette gjør det vanskelig for andre å kunne ”gjette” seg til engangspassordet.

Flere nettbanker bruker i dag engangspassord i sine innloggingsprosedyrer for å få en sikker autentisering av brukeren etter at den har oppgitt tradisjonelt brukernavn og passord. Det kan benyttes ”passordkalkulatorer” som genererer et passord der og da, eller det kan være kodekort med på forhånd ferdiggenererte engangspassord. I noen tilfeller blir engangspassord kombinert med bruk av mobile løsninger som for eksempel mobiltelefon.

## 5.2. Noe en har (tokens)

Beskrivelse av autentiseringsmetoder som baserer seg på noe som brukeren har (på engelsk kalt for ”token” - direkte oversatt til norsk blir det ”tegn”). En token er enkelt sagt noe som er unikt for en

bruker eller for en gruppe brukere. Eksempelvis er førerkortet en slik tokens for alle som har lov til å kjøre bil.

Tokens som er utviklet for å benyttes i autentiseringsprosesser er kodet med en eller annen form for informasjon (kan også være dynamisk informasjon som blir generert ved en autentisering) som benyttes i autentiseringsprosessen for å identifisere "eieren" av den gitte token.

### 5.2.1. PKI

Enkelt forklart kan man si at PKI er et opplegg for elektronisk legitimasjon og signatur. En digital signatur kan benyttes til å "signere" digital informasjon på "samme måte" som en håndskreven signatur benyttes til å undertegne et papirdokument. På samme måte kan denne funksjonen også benyttes til å autentisere brukeren overfor et system.

Et digitalt sertifikat er enkelt sagt legitimasjon i elektronisk form. Et digitalt sertifikat benyttes særlig over åpne nett (som Internett) for å bevise at man er den man gir seg ut for å være. Digitale sertifikater benyttes også for å kontrollere at en digital signatur er en gyldig og ekte signatur, og ikke en forfalsket digital signatur. Rent teknisk er et sertifikat rett og slett en fil, som eksempelvis kan oppbevares på PC-ens harddisk eller på et smartkort som brukeren får utdelt.

### 5.2.2. Smartkort

Et smartkort er et fysisk plastkort (standard kortstørrelse) og en liten datachip. I denne chip'en er det mulig å legge inn enkle operativsystem (for eksempel MultOS) som gjør at "små og enkle" programmer kan lastes ned på smartkortet og kjøres slik det gjøres på en vanlig PC. Når kortet er i kontakt med en kortleser, vil chipen få tilført strøm slik at operativsystemet aktiveres og programmer kan kjøres.

I forbindelse med PKI vil smartkortet inneholde det digitale sertifikatet som benyttes i autentiseringen. I tillegg til at autentiseringen baserer seg på et sikkert utstedt digitalt sertifikat vil også autentiseringen benytte seg av faktoren "noe som brukeren har", nemlig det fysiske smartkortet.

Det er også muligheter for at en smartkort kan inneholde en slags signatur som er utstedt av en eller annen virksomhet for at en gitt brukes på en sikker måte skal kunne identifisere seg. For eksempel kan det nevnes at Norsk Tipping benytter smartkort i forbindelse med spill over Internett. I dette tilfellet blir smartkortet utstedt til en bruker etter at han har registrert seg hos Norsk Tipping med nødvendig

informasjon. Hos Norsk Tipping blir smartkortet ikke å regne som et digitalt sertifikat, men heller som en elektronisk ID som beviser at du er den som du har opplyst at du er. En slik elektronisk ID vil være juridisk bindende på samme måte som en tradisjonell håndskreven signatur.

Framfor et dedikert smartkort som nøkkelbærer kan mobiltelefonen være et attraktivt alternativ. Mobiltelefonen er en gjenstand et stort flertall bærer med seg så å si hele tiden og benyttes allerede for kommunikasjon. Ved å integrere smartkort-funksjonaliteten i mobiltelefonen unngår man også behovet for ekstra hardware i form av smart-kortleser.

### 5.2.3. Software-basert

Istedenfor å legge et digitalt sertifikat (eller annen type informasjon som kan brukes i en autentiseringsprosess) i et fysisk smartkort er en annen løsning å legge et digitalt sertifikat inn i en software løsning. Da kan det digitale sertifikatet ligge som en fil på en PC som benyttes når det er behov for det. Innen helsevesenet ved for eksempel et labsvar vil det kunne være aktuelt å benytte seg av en softwarebasert PKI-løsning som gjør at virksomheten som er ansvarlig for labsvarene har et digitalt sertifikat som blir lagt ved labsvaret. At sertifikatet er lagret på PC'en og tilgjengelig for systemet kan medføre en større risiko for at sertifikatet kommer på avveie.

### 5.2.4. Mobile løsninger

Mobile løsninger for autentisering er i den senere tiden blitt tatt i bruk i ulike systemer. Først og fremst i forbindelse med at passord blir sendt i SMS-meldinger til en bestemt mobiltelefon. Denne formen for autentisering er blitt aktuell gjennom at mobiltelefonen er blitt allemannseie slik at det ikke krever noe ekstra utstyr for denne typen autentisering. Ofte er det engangspassord som blir sendt via SMS etter at en først har autentisert seg ved brukernavn og passord.

I tillegg til å motta et engangspassord ivaretar en mobil løsning på en måte også faktoren med ”noe en har”. En mobiltelefon er å betrakte som allemannseie samtidig som at ingen vil miste uten en da vil stoppe abonnementet som er på telefonen. På denne måten sikrer en seg om at et engangspassord sendt til en mobiltelefon med stor sannsynlighet havner hos den som også er eier av mobiltelefonen.

Andre typer for autentisering ved hjelp av engangskoder er også å betrakte som mobile løsninger. Disse baserer seg da for eksempel på ”passordkalkulatorer” som brukeren har fått utdelt slik at brukeren gjennom slike enheter får en engangskode som må oppgis ved autentiseringen.

Mobiltelefonen kan også benyttes sammen med digitale sertifikater lagret på telefonen, noe som gir en PKI basert på mobiltelefonen. Fordelen med dette vil være at infrastrukturen for sikre nøkkelbærere allerede er tilstede hos et stort publikum.

### 5.3. Noe en er (biometriske løsninger)

Noen menneskelige fysiske egenskaper er unike for hvert enkelt menneske. Det mest kjente er vel fingeravtrykket som på en ensidig måte kan identifisere alle mennesker. Unike menneskelige fysiske egenskapene kan benyttes i autentiseringsprosesser til entydig å kunne identifisere en entydig bruker.

Biometri er målbare biologiske egenskaper som for eksempel fingeravtrykk, netthinne ellers stemmeavtrykk. Innen datasikkerhet betyr biometrisk autentisering at en benytter seg av autentiseringsteknikker som bruker fysiske egenskaper som kan kontrolleres automatisk. Biometri kan benytte både rene fysiske egenskaper (som fingeravtrykk) eller spesifikke karakteristikk ved en person (som stemme eller håndskrift).

Å benytte biometriske egenskaper til autentisering kan være en omfattende prosess i og med at brukerne må registreres i systemet med de egenskapene som skal benyttes i autentiseringen. Dette kan være fingeravtrykk, stemme eller andre ting, og dette er mer omfattende enn bare å gi en bruker et brukernavn og tilhørende passord. Disse egenskapene må så lagres for senere å kunne benyttes til autentisering av brukeren.

I tillegg må det også sjekkes at personen som det avhentes biometriske egenskaper fra faktisk er den som han utgir seg for å være. Det må også kontrolleres at personen skal autoriseres for tilgang til det gitte systemet (dette gjelder generelt ved autorisasjon til alle former for autentisering).

En sentral utfordring med biometrisk autentisering er å unngå feilaktig avvisning av personer som er autorisert for tilgang. Et kutt i fingeren eller endring i stemmen pga. en forkjølelse må ikke føre til at en autorisert bruker blir avvist av systemet. Dette gjør at nivået for godkjenning må senkes i forhold til hva som er mulig for å sikre seg at reelle brukere ikke blir feilaktig avvist av systemet.

En ulempe med biometrisk autentisering er at en benytter seg av noe som er unikt. Et brukernavn eller passord kan en IT-administrator lett endre dersom det er behov for det. Dersom noen greier å stjele identiteten din har du inn ingen mulighet for å endre på verken fingeravtrykk eller øyne. En kan selvfølgelig ugyldiggjøre et stjålet biometrimønster, med den virkning at verken du eller noen andre kan benytte seg av det.

Det finnes flere ulike metoder og egenskaper som kan benyttes ved biometrisk autentisering. Her er en kort oversikt over de mest vanlige:

- ❑ **Fingeravtrykk** - kanskje den mest kjente formen for biometrisk autentisering som har vært benyttet av politiet i en årrekke. Bruker mønsteret i huden på fingertuppene, som er unikt for alle mennesker, for å identifisere en bestemt person.
- ❑ **Håndgeometri** - måler og analyserer formen på hånden.
- ❑ **Øyne** – en har to former for autentisering ved bruk av øyne:
  - Iris - analyzing features found in the colored ring of tissue that surrounds the pupil
  - Retina - analyzing the layer of blood vessels situated at the back of the eye
- ❑ **Stemme** - ved bruk av stemmen til autentisering bruker en som oftest ikke tradisjonell stemmegjenkjenning, men en "voice-to-print" metode. Dette gjør at stemmen blir konvertert til tekst som kan brukes i autentiseringsprosessen.
- ❑ **Ansiktsform** - analyserer spesielle karakteristikker i ansiktet (nese, øyne, forholdet mellom ulike spesielle "trekk" i ansiktet). Krever et digitalt kamera som kan lage et "ansiktsbilde" av den som skal autentiseres.
- ❑ **Håndskrift** - ved bruk av håndskrift blir det gjort analyser av hvordan en person skriver sin egen signatur. Faktorer som hastighet og press er ting som kan identifisere en person.

## 6. Eksempler på webløsninger

Beskrivelse av to ulike løsninger for pasient-lege kommunikasjon over Internett hvor det er høye sikkerhetskrav til autentisering av brukere (pasientene).

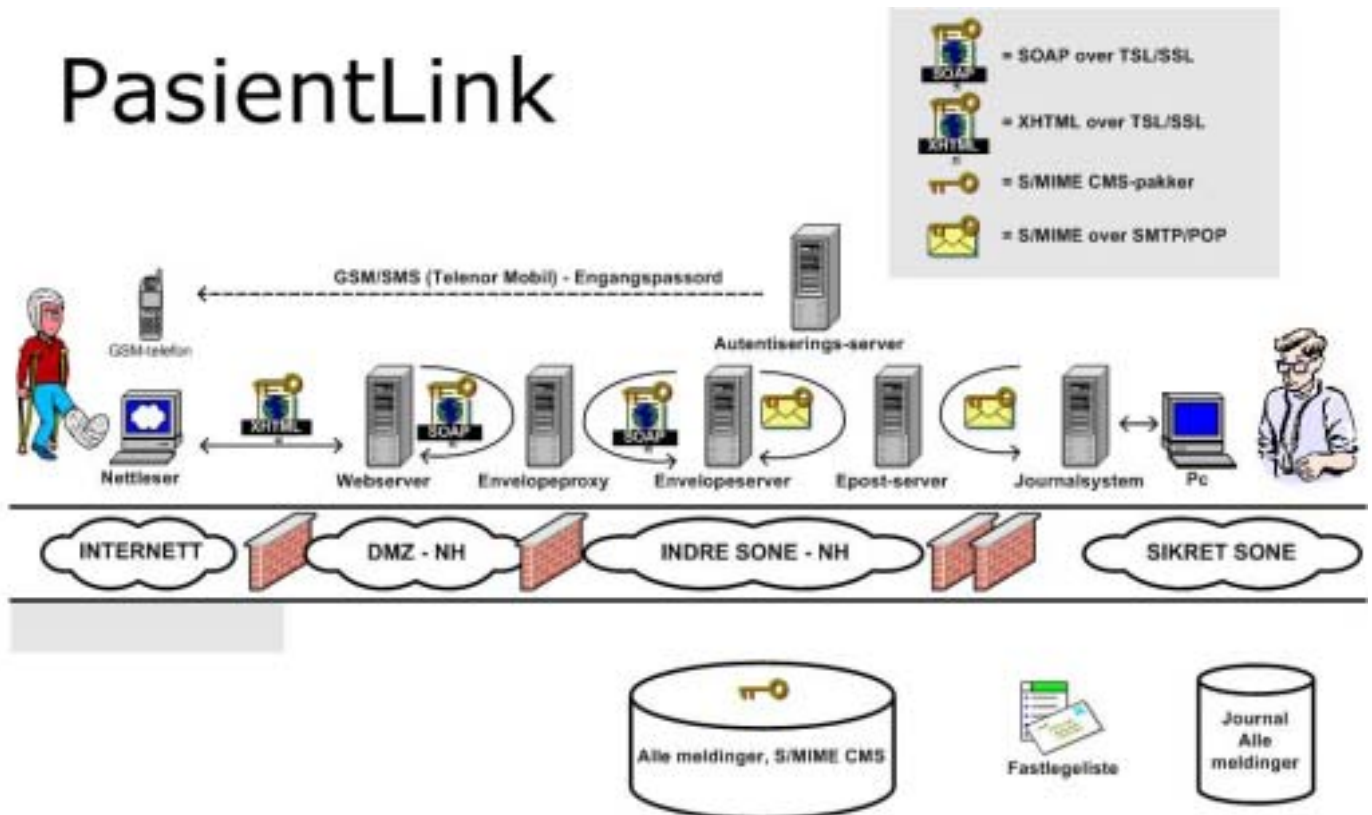
### 6.1. PasientLink

PasientLink er et system utviklet av NST (Nasjonalt Senter for Telemedisin) som gir pasienter mulighet til å kontakte sin fastlege over Internett. Pasientene bruker en webleser for å skrive spørsmål og lese svar. De logger seg på ved hjelp av brukernavn/passord og en engangskode som mottas via SMS. Ved utvikling av løsningen er det lagt vekt på en rekke faktorer:

- Løsningen skal tilfredsstillere lovpålagte krav til informasjonssikkerhet. Dette gjør at tradisjonelle e-post baserte løsninger er lite egnede.
- En form for to-fase autentisering kreves som adgangskontroll. Dette utelukker en løsning basert kun på passord. Typisk må man benytte seg av en tilleggsenhet som for eksempel et smartkort eller en kodekalkulator. I PasientLink benyttes en mobiltelefon.
- Løsningen skal være svært billig per pasient. Enhetskostnaden med å legge til nye pasienter må ikke være høyere enn en vanlig egenandel ved et legebesøk. Dette utelukker løsninger som krever installasjon av fysiske enheter hos pasientene, og det gjør det også nesten umulig å basere seg på løsninger som krever installasjon av programvare (p.g.a kostnadene av support).
- Løsningen skal gjøre det mulig å sende tekst begge veier. Multimedia og skjema bør støttes på lengre sikt

Prosjektet har utviklet en egen modul for autentisering vha. engangspassord overført via SMS som er tilgjengelig som åpen kildekode.

# PasientLink



Figur 1: skisse over PasientLink (Kilde: <http://www.telemed.no/cparticle58176-7457.html>)

Modulen kalles SMSAuthenticator. Autentiseringen starter med at pasienten skriver inn en angitt Internett-adresse i webleseren. Denne internettforbindelsen er kryptert ved hjelp av https (Secure Hypertext Transfer Protocol). Deretter kan pasienten logge seg inn ved hjelp av brukernavn og passord. Dersom dette godkjennes av autentiseringsserveren blir en engangskode sendt via SMS på mobiltelefon. Denne engangskoden, som er gyldig i 5 minutter fra den ble sendt, blir så brukt i andre fasen av autentiseringen sammen med brukernavnet til pasienten.

I tillegg til autentiseringen benyttes andre protokoller for å sikre kommunikasjonen mellom pasient og lege.

## 6.2. medAxess

medAxess er en løsning utviklet av Deriga som utprøves i Midt-Norge i samarbeid med Midt-Norsk Helsenett. Også denne løsningen er utviklet med tanke på kommunikasjon mellom lege og pasient over Internett.

Gjennom medAxess kan pasienter:

- Bestille time
- Søke om resept
- Søke om legeattest
- Sende andre enkle meldinger til legen

Utenom dette tilbyr medAxess funksjonalitet slik at legen kan svare på henvendelser fra pasienter samt et administrasjonsverktøy for nettstedet.

## Referanseliste

- [1] The open web application security project – A guide to building secure web applications
- [2] National Institute of Standards and Technology – “FIPS 190 - GUIDELINE FOR THE USE OF ADVANCED AUTHENTICATION TECHNOLOGY ALTERNATIVES”
- [3] Nasjonalt senter for telemedisin – Pasientlink – teknisk beskrivelse av løsningen
- [4] Jan Wolter - A Guide to Web Authentication Alternatives
- [5] Matthew D. Ford, BT Laboratories Ipswich – Identity Authentication and “E-commerce”