TEKNOLOGI-RÅDET

Plastkort som borgerkort

Anvendelse af ic-kort teknologien til borgerkort

TeknologiNævnets rapporter 1994/2
Projektleder i Teknologinævnets sekretariat:
Lars Klüver

Steffen Stripp
Teknologinævnet, København 1994

Indholdsfortegnelse

b) Personlige beviser
c) Generel helbredsjournal
d) Specialiseret helbredsjournal
e) Vandrejournal i sundhedssektoren
f) Recepter/medicinforbrug
g) Nød-/advarselsoplysninger
h) Arbejdsløses sagsjournal
i) Arbejdsløses vandrejournal
j) Uddannelsesdata

4.G Brugerbetaling

a) Penge
b) Administrations-regler
c) Vejafgifter

5. Sikkerhed

a) Kvalitetskrav
b) Scenarier
c) Kortet
d) Kortindehaver identifikation
e) Kortlæser
f) Datakommunikation

6. Brugbarhed

a) Kvalitetskrav
b) Kunne bruges af alle
c) Valg af anvendelse og data
d) Forstå anvendelsen

7. Vurdering

7.A Funktionel vurdering

a) Systemudformning og projektgennemførelse
b) Vurdering af anvendelses-eksemplerne
c) Hvilke borger ic-kort?
d) Privatkort

7.B Økonomisk vurdering

7.C Etiske vurderings-kriterier

a) Deltagelse i elektronisk kommunikation
b) Privat elektronisk kommunikation
c) Robust samfund
d) Persondata-beskyttelse
e) Individets kort
f) Anvendelsen frivillig
g) Frivillig personlig legitimation

8. Høringssvar

Indenrigsministeriet - CPR-kontoret
Finansministeriet
Kommunernes Landsforening
Amtsrådsforeningen i Danmark

Forord

Denne rapport er resultatet af et projekt, gennemført i Teknologinævnet i perioden februar 1993 til juli 1994.

Projektet blev påbegyndt før danskerne fik et plastikkort, som kan betegnes som et borgerkort. Men udviklingen har ikke stået stille, mens projektet har kørt. Siden projektets start har vi fået et plastsygesikringsbevis og Indenrigsministeriet har i februar 1994 igangsat et forprojekt om et elektronisk borgerkort. Det er med andre ord i projektperioden blevet tydeligt, at der er behov for analyse og debat på området.

Denne projektrapport vil kunne anvendes som grundlag for stillingtagen i debatten om de initiativer - eller mangel på samme - som EU, staten, amter, kommuner og private virksomheder står bag.

Projektet er blevet hjulpet på vej af mange mennesker, som Teknologinævnet ønsker at takke for deres indsats. Først og fremmest konsulent Steffen Stripp, som har stået for udredningsdelen og har skrevet projektrapporten. I det arbejde har han trukket på mange hjælpsomme ressourcer og har oplevet stor åbenhed i virksomhederne, som opererer på området. Referencegruppen, som har bestået af Oluf Jørgensen, Morten Lindstrøm, Henrik Bonde Nielsen og Søren Olesen, har kommenteret mangfoldige udkast og skal have en særlig tak for deres anstrengelser. Endelig skal interessentgruppen takkes.

Konsensuskonferencen, som var en del af projektets vurderingsfase, blev ledet af Carsten Schnack, som har ydet en stor indsats, både som ordstyrer og som lægpanelets formand. Sidst, men absolut ikke mindst, skal lægpanelet takkes for at have deltaget ivrigt og konstruktivt i arbejdet - til langt ud på natten.

Rapporten og dens konklusioner er ikke udtryk for Teknologinævnets holdninger, men skal betragtes som resultatet af den proces, som projektet har været. Konklusionerne må derfor betragtes som et udtryk for lægpanelets, interessenternes og projektledelsens samlede indsats.

Det er Teknologinævnets håb, at denne rapport vil sætte sit præg på Danmarks anvendelse af borgerkort fremover.

Teknologinævnet, august 1994.

1. Hvorfor udredning om et ic-kort som borgerkort?

Baggrunden for "udredning om ic-kort som borgerkort" er et forventet fremtids-scenario, som viser, at danskerne vil få plastkort som borgerkort. Dette scenario kan forudses ud fra to udviklingstendenser: kortene forberedes, og er på vej og den stadig øgede anvendelse af elektronisk informations-teknologi fører frem mod, at alle bliver inddraget i elektronisk kommunikation med offentlige myndigheder og private virksomheder.

Ic-kort

Et ic-kort er et plastkort, i samme format som et Dankort. I stedet for magnetstriben er der indbygget en computer i kortet, selv om det umiddelbart kan forekomme nærmest umuligt i et plastkort som er 0,76 mm tykt. Kortet kunne kaldes for et computer-kort, men betegnes i internationale standarder som et ic-kort. Computeren er en integreret kreds, integrated circuit, som har givet navn til kortet. En integreret kreds på en silicium skive kaldes for en chip, og kortet omtales også som et chip-kort. Endelig omtales et ic-kort ofte med et mere markedsføringspræget udtryk som et smart-kort.

a) Borgerkort på vej

Danskerne har gennem de senere år vænnet sig til plastkortene. Plastkortet med magnetstriben kendes fra Dankortet og en lang række andre betalingskort. Ic-kortet er først nu på vej ud til danskerne. Nogle få har mødt det ved adgangskontrol til deres arbejde. Danmønt, et småpenge ic-kort til telefoner, automater og lignende, er efter et pilotforsøg i Næstved i 1993 på vej til en udbredelse i hele Danmark. I GSM mobiltelefonen benyttes et ic-kort til at identificere hvem der ringer op og skal betale regningen. I Storstrøms Trafikselskab (STS) introducerer man ic-kort som klippekort til busserne.

Udvikling af sygesikringsbeviset, et nyt cpr-bevis eller et id-kort og udstedelse af et servicekort har været behandlet i flere omgange hos forskellige offentlige myndigheder siden midten af 70-erne. Det første borgerkort fik danskerne i 1994 med plast-sygesikringsbeviset.

Plast-sygesikringsbevis

Plast-sygesikringsbeviset har samme formål som det hidtidige pap-bevis, at være en dokumentation for ret til ydelser fra sygesikringen. Det har en udvidet anvendelse ved at kunne overføre navn, adresse og cpr-nummer på forskellig måde, herunder elektronisk fra magnetstriben.

I den rapport [1] som anbefalede plastsygesikringsbeviset forestiller man sig dog en bredere anvendelse. En "generel udstedelse af plast-sygesikringsbeviser vil medføre en mere udbredt anvendelse af plastsygesikringsbeviset i den kommunale administration samt hos andre offentlige myndigheder ved udfyldelse af bilag." (s. 74)

Sammenfaldet mellem et forsøg med kortet i to kommuner og den daværende egenbetalingsgrænse ved medicinkøb, som indebar, at patienter selv skulle afholde 800 kr. af udgifterne til tilskudsberettiget medicin, viste at plastkortet kunne anvendes til administration af brugerbetaling.

Endvidere fremlægger den nævnte rapport overvejelser om sammenhængen med andre beviser. "På det kommunale område udstedes f.eks. medicinkort til pensionister, buskort og lånerkort til folkebibliotekerne. Amtskommuner anvender i stor udstrækning beviser indenfor sygehusvæsenet. De enkelte sygehuse udsteder således beviser ved patientregistreringen, der følger patienten under sygehusopholdet. Endvidere kan nævnes et særligt bloddonorbevis. /../ Staten udsteder hvert år et skattekort til samtlige skattepligtige borgere." (s. 19) Og man opsummerer "Plastkortets muligheder for at kunne påføre oplysninger elektronisk på plastkortets magnetstribe åbner mulighed for, at kortet på et senere tidspunkt kan anvendes som buskort, medicintilskudskort, bloddonorkort m.v." (s. 63)

Sundhedskort

I et forslag til lov om det offentlige sundhedsvæsen [2] foreslås, at der indføres et generelt sundhedskort. Forslaget bemyndiger sundhedsministeren til at fastsætte nærmere regler om udformning, indhold, udstedelse og inddragelse af sundhedskort. Det

hedder i bemærkningerne: "Sundhedskortet kan tillige åbne mulighed for med de berettigedes samtykke at registrere vigtige helbredsoplysninger om f.eks. kroniske sygdomme, allergier, blodtype, vaccinationer, samt eventuelle organdonortilsagn til brug under akutte omstændigheder."

I en rapport fra Finansministeriet [3] behandles et eksempel på anvendelse af et sundhedskort, der teknisk er et ic-kort.

Under et ferieophold i Danmark får Hansen brug for en vagtlæge: "I chippen på Hansens sundhedskort findes en række stamoplysninger om blodtype og lignende samt en kopi af den journal, som Hansens egen læge fører på sit edb-udstyr."

"Ved hjælp af sit bærbare lægesystem og Hansens sundhedskort får lægen over det offentlige datanet adgang til at læse Hansens sygehus-journal ... Hansen foretrækker dog at få recepten udleveret. Ved hjælp af den bærbare (pc) skriver lægen derfor en recept i chippen på Hansens sundhedskort ... På apoteket aflæses recepten i chippen på Hansens sundhedskort."

Servicekort

Ekstrabladet kunne den 9. juli 1988 omtale et notat fra Finansministeriet, Indenrigsministeriet og Sundhedsministeriet med overskriften "Budgetanalyse vedrørende servicekort".

Ministerierne har ikke ønsket at udlevere notatet. Det hedder her fra kopi i Ekstrabladet:

"Der udstedes et servicekort til alle borgere i Danmark. Servicekortet erstatter bl.a. de nuværende CPR- og sygesikringsbeviser. Kortet vil indeholde de oplysninger, der idag fremgår af sygesikringsbeviserne, og borgerne vil herudover have mulighed for at tilføje personlige oplysninger f.eks. blodtype, organdonor mv. på kortet.

Kortet tænkes fornyet årlig, og i forbindelse hermed opkræves et årligt fornyelsesgebyr. /../ Der indføres endvidere mulighed for at få en række "tillægsydelser" mod betaling af et årligt gebyr. Det drejer sig om følgende områder

- vagtlæge- og skadestuebesøg uden for almindelig arbejdstid
- rejsesygesikring
- tilskud til tandlægeydelser
- forebyggende helbredsundersøgelser
- lån af bøger
- fisketegn"

I tilknytning til registeret foreslås et servicekort-register i Indenrigsministeriet med adgang til hvilke tillægsydelser borgeren har adgang til, mens sygesikringsdata fortsat opbevares i sygesikringsregisteret.

I en udsendelse i DR-TV den 27. januar 1994 blev det oplyst, at der i 1991 blev foretaget en fornyet intern budgetanalyse om udstedelse af et servicekort.

Internationalt

Ic-kort anvendes i mange forskellige sammenhænge i en lang række lande. Studerende har et kort med deres eksamenskarakterer for at undgå snyderi (Italien). Kommunens borgere har adgang til et kort som kan bruges til identifikation, betaling og evt. personlig prisreduktion i svømmehallen, parkering, vejafgifter, museer m.m. (Finland). Social bistand udbetales på et ic-kort, der kan anvendes i bestemte butikker til indkøb (USA). Nyfødte får et ic-kort med deres navn på, hvor der kan opbevares helbredsdata om vægt, højde, vaccinationer. (Spanien). Ic-kort er adgangskort til Singapores bymidte, er der ikke penge på kortet fotograferes nummerpladen. Osv.

De mest omfattende bestræbelser koncentrerer sig om sundhedskort og id-kort.

Sundhedskort

I Tyskland begyndte man i 1993 at udsende et ic-sygesikringskort til alle tyskere [4]. Kortet skal primært anvendes til administration af forsikringsforhold.

I Frankrig anvendes ic-kort til at opbevare administrative data og helbredsdata.

I EU arbejdes der inden for AIM-programmet intenst på at udvikle forskellige sundhedskort. Et projekt har udarbejdet et særligt kort for diabetikere, DIABCARD [5]. En konsulent-rapport har fremlagt overvejelser om en strategi for sundhedskort [6].

I det europæiske standardiseringsorganisation (CEN) er nedsat en særlig arbejdsgruppe om sundhedskort (TC251/WG7 hedder den).

ID-kort

Alle borgere i Tyskland har et særlig id-kort (Personalausweis), som man har pligt til altid at bære på sig. Kortet er udformet som et plastkort. Kortet har ud over billede og underskrift følgende personoplysninger:

- efternavn, evt. fødselsnavn og fornavne,
- stillingsbetegnelse (doktorgrad),
- fødselsdato og fødested,
- størrelse og øjenfarve.

Desuden har beviset en zone for automatisk aflæsning af fødselsdato og et serienummer.

Sammen med id-kortet er der oprettet et særligt centralt register, Personalausweisregister. Loven om personlegitimation tillader bl.a. at myndighederne kan forbinde plastkortet med registeret for at kontrollere landets grænser eller for at finde efterlyste personer [7].

I Australien har den socialistiske regering fremført et forslag om et generelt identifikationskort - The Australian Card [8]. Forslaget blev genstand for en større politisk kamp og blev ikke gennemført.

Indførelsen af kortet var fra starten snævert knyttet til etablering af et centralt personregister.

Kortet skulle indeholde en række personoplysninger, bl.a.:

- navn
- identifikationsnummer
- foto og underskrift
- andre autentifikationselementer og sikkerhedstiltag.

Indholdet i registeret blev defineret i loven som minimum følgende:

- navn
- fødselsdato
- køn
- aktuel adresse
- titel
- status som australsk borger eller anden status
- ret til offentlige sundhedstjenester
- arbejdstilladelse
- navn ved fødsel eller indrejse
- andre navne som anvendes
- adresser de seneste to år
- kortnummer
- dødsdato
- dokumenter brugt til at etablere identitet
- detaljer i forbindelse med ansøgning om kort
- et digitaliseret foto af kortindehaveren
- en digitaliseret underskrift.

En række af disse oplysninger findes også i danske personregistre, men for en række oplysninger går man langt videre, f.eks. digitaliseret foto og underskrift. Forslagets kritikere hævdede, at der kun var tale om en begyndelse.

Kortet blev oprindelig foreslået for at bekæmpe skattesnyderi. For at nå dette mål skulle kortet være nødvendigt ved alle banktransaktioner inkl. hævninger fra egen konto eller adgang til egen bankboks, alle transaktioner i forbindelse med ejendomshandler, al aktiehandel, ansættelser, behandling på sygehus eller krav om sygepleje.

Fra England rapporteres om planer om identifikations-kort på ic-kort. En undersøgelse skal have vist at 78% af den britiske befolkning vil acceptere et ID-kort for at forebygge terrorisme. Test af id-kort, som benytter ic-kort teknologien, er startet i Frankrig og USA [9].

I Schiphol Lufthavnen i Amsterdam anvendes et ic-kort, som indeholder et elektronisk billede af personens fingeraftryk, til identitets-kort. Ved anvendelse af kortet til en automatisk identifikation kan rejsende opnå en hurtigere passage i lufthavnens kontrol. Ved kontrollen sker der automatisk opslag i Schengen-registeret, som indeholder data om efterlyste personer [10].

b) Elektronisk kommunikation en del af hverdagen

Iflg. en undersøgelse har 92% af alle danske familier et betalings-kort [11], og danskerne kommunikerer daglig elektronisk når de benytter betalingskortene. 2,3 millioner danskere har et Dankort og benyttede det i 1992 127 millioner gange i pengeautomater, restauranter, nota-systemer og i butikkernes kasseterminaler [12]. Brugen af plastkort og håndtering af en dagligdags foreteelse, betaling, er almindelig udbredt.

Der sker en stigende udbredelse af elektroniske service-ydelser baseret på trykknap-telefonen. Der er tale om oplysnings-tjenester hos offentlige myndigheder og private virksomheder. Bankerne har udvidet tjenesterne til egentlige service-ydelser, hvor kunden kan gennemføre en række forskellige bankforretninger automatisk. Det er ikke kendt, hvor mange der benytter sådanne tjenester, men på grund af trykknap telefonens store udbredelse i Danmark må tallet skønnes at være stort.

Et spring i den elektroniske kommunikation bliver mulig i takt med at flere danskere får adgang til en pc i hjemmet som via modem kan kommunikere elektronisk med edb-systemer. Idag har ca 25% af alle hjem en pc, heraf har omkring 10% modem. Analyseinstituttet IDC skønner at antallet af danske husstande med pc'er vil stige kraftigt i de kommende år og at pc'en vil være ligeså almindelig som telefonen om syv år [13]. Interessen fra udbydere af elektroniske serviceydelser er så stor, at de vil tilbyde modemer til lave priser eller endog gratis. Det må endvidere forventes, at der også vil være andre billigere tilbud. Særlige terminaler af minitel-typen, som er specielt designede til at klare visse kommunikations-funktioner. I Frankrig blev de udleveret gratis i stedet for telefonbøger. En anden mulighed er en såkaldt smart telefon, der i stedet for de kendte knapper, har en berøringsfølsom skærm, som skifter knapper efter behov og kan vise udskrifter fra kommunikationen.

På sikkerhedssiden vil ic-kort med eller uden betalingsfunktioner og forskellige former for elektronisk underskrift give den sikkerhed som kan gøre anvendelse af kommunikation fra hjemmet mere og mere naturlig [14].

Der vil i de kommende år komme et stort udbud af elektroniske service-ydelser, som den enkelte kan benytte. Diatel, som er en virksomhed der vil udbyde informations-serviceydelser fra 1994, nævner som eksempler: bankforretninger, forbrugerinformation og indkøb, aviser og nyheder, telefonbog, spil - f.eks. tips og lotto - og aktiviteter, foreninger, kommuneinformation.

Endelig vil borgerne have mulighed for at sende elektroniske brev til hinanden, og til virksomheder og myndigheder. Det er en hurtig og billig måde at kommunikere på.

c) Manglende helhedsvurdering

Anvendelser af ic-kort er mangfoldige og de ideer, der lægges frem er ofte utrolige. Ideer om at man har alle sine personlige oplysninger i en databank på ét kort nævnes og på den anden side omtales muligheder for et effektivt id-kort.

På trods af de mange ideer og de stadig flere praktiske anvendelser af ic-kort er der ikke gennemført helhedsprægede teknologi-vurderinger af, hvad vi hensigtsmæssigt kan bruge denne teknologi til.

Institut for Fremtidsforskning gav i et lille projekt for en kortleverandør, der blev offentliggjort i to artikler i Berlingske Tidende [15], nogle bud på anvendelser:

- De centrale "registre vi kender, som har grundlag i de store edb-centraler fra 60'erne kan nu opbevares på smart-kort, hvis anvendelse borgerne selv kontrollerer".

- "Den meget høje grad af sikkerhed ved smart-kortet gør, at det med fordel kan erstatte traditionelle nøgler".

- Smart-kortet kan erstatte sygejournaler.

- Særlig et område "har fanget opmærksomheden: anvendelse i relation til brugerbetaling i det offentlige." Smart-kortet giver meget varieret mulighed for "indførelse af brugerbetaling med socialt sigte."

Instituttet sammenfatter: "Har erhvervslivet og politikerne det nødvendige initiativ og visionerne kan Danmark gå hen og blive et foregangsland i anvendelsen af smart-kortteknologien, sådan som vi faktisk allerede er det med Dankortet. Det kan på lang sigt medvirke til at styrke både den offentlige sektors finanser, individets sikkerhed mod overvågning og kontrol og vores konkurrenceevne inden for højteknologi."

Der er også kritiske røster. Jon Bing advarer på baggrund af The Australian Card: "Man ser her let kimen til et universelt flerbrukskort som ville legge elektroniske spor nær sagt overalt, og gjøre samfunnet svært gennemsiktig sett fra den myndighet som samler opplysningerne /../ historien om Australia Card tydeliggjør sammenhengen mellom sentralt personregister og bruk av identitetskort, og antyder hvilke muligheter en slik sammenkobling kan åpne. Enkelte av disse mulighetene er fristende, og derfor kan de nordiske land, med sine omfattende sentrale befolkningsregistre og den høyt automatiserte offentlige forvaltning også gi grobunn for en politikk som tillater større kontroll med privatøkonomi, f.eks. for å komme skatteunnvikelser til livs." (Artiklen omtalt ovenfor, s. 73)

Ser vi på eventuelle danske borgerkort er det både ud fra demokratiske, effektivitetsmæssige og samfundsøkomiske betragtninger nødvendigt med en helhedsvurdering af denne teknologi før borgerkortet udsendes. Det er f.eks. betænkeligt, at man lægger op til at sygesikringsbeviset glidende skal ændres til et id-kort i forskellige sammenhænge. Er det overhovedet egnet til det?

[1] Amtsrådsforeningen i Danmark (red. Lars Toft): Videreudvikling af sygesikringsbeviset (1990)
[2] Lovforslag L74 af 30. oktober 1991.
[3] Finansministeriet: "Effektiv edb i staten" (1992). Bilag 3: "Datafællesskaber - koordination af dataudveks ling på tværs af organisationer": "Scenario om sundhed - et eksempel på datafællesskaber" s. 28-29.
[4] Card Technology Today May 1993
[5] EF-kommissionens blad XIII Magazine: Patient Data Cards. August 1993.
[6] Cap Sesa: Preparation of a European Strategic Action for the use of "Data Cards" in the Health Care Domain. (1993)
[7] Gesetz über Personalausweis.
Omtale i Kirsten L. Jensen og Henrik Schneider: Visioner om Informationssamfundet. (1986)
[8] Jon Bing: Bruk av identifikasjonsbevis. I Jon Bing og Jørgen Fog: Fem Essays om ny information steknologi, forbrukere og personvern. NEK rapport 1989:3
[9] Virus News International October 1993: British Police Formulating Plans for Smart Card ID Cards.
[10] Virus News International, op.cit. Udklip Hollandsk dagblad
[11] Undersøgelsen er foretaget af Payment Service International over udbredelsen af betalingskort i Europa (1993).
[12] ComputerWorld nr. 44-17.december 1993.
[13] ComputerWorld nr. 32-24. september 1993 og nr. 3-21.januar 1994.
[14] Johannes Luef (innovationschef PBS): Homebanking og homeshopping. Dataposten 3-93
[15] Christian Lotz og Uffe Paludan: Det registerløse samfund.
Berlingske Tidende 28/6-89. Og Brugerbeta ling i et pengeløst samfund. Berlingske Tidende 29/6-89.

2. Udredningen

Denne udredning om "ic-kort som borgerkort" skal på baggrund af konkrete analyser af anvendelser og udvikling af vurderingskriterier give grundlag for en helhedspræget vurdering af et multifunktions ic-kort i en fremtid, hvor borgerne indgår i elektronisk kommunikation og databehandling. Formålet med udredningen er:

* at skabe et helhedsorienteret grundlag for en evt. indførelse af et borger ic-kort
* at afdække borger ic-kortets konsekvenser for borgernes stilling i samfundet
* at styrke opmærksomheden overfor fremtidssikrede løsninger og derigennem at bidrage til, at fejltagelser undgås og penge spares.

a) Teknologivurdering

I Teknologikritik - et teknologifilosofisk essay, opdeles diverse kritikformer i tre typer [16].

Vurdering der handler om at placere en teknologi som ønskværdig/uønsket, god/dårlig, rentabel/urentabel osv. En mere fundamental, *kategorial kritik* forekommer, hvis spørgsmålet ikke drejer sig om hvilke begreber man vil hæfte på teknologien, men om begrebstyperne overhovedet kan bruges. En tredje kritikform, *objektiv kritik*, handler ikke om grænsedragninger, men om selve objektet for kritikken. "Den vurderende kritik retter sig på sin vis også mod en genstand, men søger netop (blot) at vurdere den. Den objektive kritik søger at gribe ind og ændre selve genstanden for kritikken. Medens den vurderende kritik søger den rette beskrivelse/vurdering af sin genstand, søger den objektive kritik netop den "rette" genstand" (s.100f).

I denne opdeling kan udredningen placeres som en vurdering af en teknologi. En konsekvens er, at forhold uden for undersøgelsens genstand tages for givet. Det tages f.eks. for givet, at der i fremtiden vil være en udbredt brug af elektronisk kommunikation, og der spørges ikke om en sådan udvikling er fremmedgørende for mennesker, eller om homebanking og homeshopping er et godt tilbud til forbrugerne.

"Der er mange mulige definitioner på teknologivurdering. Men i sidste ende handler det om systematiske og alsidige vurderinger af de samfundsmæssige og menneskelige konsekvenser af eksisterende og ny teknologi" [17] . Borger ic-kort er ikke udsendt til danskerne, der ligger endog ikke konkrete forslag fra myndighederne på bordet. Udredningen bygger, som beskrevet i afsnit 1, på den antagelse, at vi vil få borger ic-kort i fremtiden. Udredningen er et fremtidsstudie, der beskriver mulige fremtidige anvendelser af ic-kort som borgerkort. Det er således ikke målet at forudsige, hvordan fremtiden vil se ud, men at give et grundlag for at gøre valg og tage beslutninger.

Udredningens genstand er et evt. kommende edb-baseret system. Systemet kan beskrives som et borgerkort-system med anvendelse af ic-kort teknologien. Der er således ikke tale om en vurdering af ic-kort teknologien i almindelighed, men om en vurdering af ic-kort i en bestemt type systemer, borgerkort-systemer. Et borgerkort-system er ikke interessant i sig selv. Det er først når det virker sammen med andre typisk edb-baserede systemer, det får en praktisk anvendelighed. Dankortsystemet er interessant, fordi det virker sammen med bankernes øvrige edb-systemer, og dermed kan bruges til betalinger. Udredningen må derfor inddrage sådanne andre systemer, som borgerkort systemet kommunikerer med og bliver et fælles system med. Men det øvrige system inddrages kun for at belyse mulige anvendelser for et borger ic-kort. Konstateres det, at ic-kort teknologien ikke er et relevant bidrag til en løsning i systemet, afsluttes analysen her. Hermed er der ikke sagt noget om hvorvidt problemet er reelt eller om der måske kan findes andre edb-løsninger.

Mens udredningen er begrænset i forhold til hvad der vurderes, er den søgt mest mulig åben i forhold til mulige borger ic-kort systemer. Der er indsamlet materiale for at belyse alle tænkelige anvendelser for et borger ic-kort og det er blevet overvejet om de kan samles på ét borgerkort. Vurderingen er helhedsmæssig ved udover funktionelle vurderinger, at inddrage sikkerhed og brugbarhed, supplere med en økonomisk vurdering og endelig - og vigtigst - ved at fremlægge etiske overvejelser.

Konsekvenserne af en ny teknologi som et borger ic-kort kan ikke fuldt ud forudsiges. Kunne de det, var der ikke tale om noget nyt. Vil vi have forandringen, må vi "acceptere en risiko, som kan beregnes [18] og en usikkerhed, som ikke kan beregnes." Vi må skelne mellem fire forskellige situationer:

1 Situationen er præget af sikkerhed, idet vi kender udfaldet af en handling.
2 I den anden situation er der tale om risiko, idet vi ikke er fuldstændig sikre, men mener dog vi kender de mulige udfald og sandsynligheden for at de indtræffer.
3 Situationen bliver usikker, hvis vi godt nok kender de mulige udfald, men ikke kan sige noget om sandsynligheden for at de indtræffer.
4 Endelig kan situationen karakteriseres som uvidenhed, hvis vi ikke engang kender de mulige udfald. (s75f)

Udredningen kan ses som et bidrag til at flytte vores situation fra uvidenhed op mod sikkerhed. Udgangspunktet for arbejdet var en nærmest total forvirring om mulige anvendelser og konsekvenser. Det første trin i udredningen har derfor været at skabe klarhed over hvilke anvendelser, der, set fra en funktionel vinkel, overhovedet er reelle. På den måde var det tanken at skabe nogle scenarier for fremtidige borger ic-kort. Men den funktionelle vurdering endte op med nogle få mulige borgerkort, hvoraf ét, privatkortet, fremlægges til en bredere debat. Vi er på den måde gået fra en noget tåget debat præget af uvidenhed til en debat i en usikker situation. Med udredningens forslag om et privatkort kender vi et borgerkort, men hvad vil det betyde for os? Her findes ikke endelige svar. Gennem en række etiske overvejelser skabes for det første grundlag for, at man kan forholde sig åbent debaterende til usikkerheden. Og for det andet for at man kan overveje beslutninger, som reducerer usikkerheden. Der er en usikkerhed både ved en fremtid med privatkort og en fremtid uden. Opgaven kan derfor siges at være at tage beslutninger så vi vælger fremtiden med den mindste usikkerhed.

b) Fremgangsmåde

Projektet er forløbet i tre faser: udredning, evaluering og endelig anbefaling og slutformidling.

Udredningen

Udredningen er gennemført med en række sammenhængende aktiviteter:

Anvendelses-eksempler

Analyse af en lang række mulige anvendelser af ic-kortet. Det er sket ved indsamling af oplysninger fra brugere, rapporter, standardiserings-oplæg, artikler mv.

Arbejds-sessioner

Der er afholdt tre heldagsmøder om sikkerhed, tekniske muligheder og etiske og retssikkerhedsmæssige spørgsmål. En oversigt med de personer, der har deltaget i møderne findes i afsnittet: Referencer.

Interessentgruppe

Ved projektets opstart blev der etableret en interessentgruppe, som på en række møder har kommenteret arbejdspapirer og ideer fra projektet. Deltagere i interessent-gruppen er listet i afsnittet: Referencer.

Kontakter og formidling

Gennem hele udredningen har der været mange kontakter med enkeltpersoner, virksomheder og organisationer. Projektet har løbende været diskuteret med en referencegruppe og er formidlet på møder og i pressen. En foreløbig version af anvendelses-eksemplerne blev sendt til udtalelse hos en række virksomheder, myndigheder og organisationer.

Vurdering

Vurderingen er for det første gennemført, som en funktionel vurdering, som afklarer hvilke borgerkort, der reelt er en mulighed. Som led i denne vurdering er udarbejdet en målanalyse, opstillet kvalitetskrav til sikkerhed og brugbarhed, analyseret mulige systemudformninger og vurderet risici ved en projektgennemførelse. For det andet er der foretaget en overordnet økonomisk vurdering. Og endelig er en række etiske problemstillinger behandlet.

Udredningsfasen blev afsluttet medio februar 1994 med en foreløbige rapport, svarende til denne rapports afsnit 1 og 3 - 7, og en særlig pjece, som fremlagde forslaget om et "privatkort".

Evalueringen

Evalueringen har bestået i tre aktiviteter:

Høring

Den foreløbige rapport blev sendt til høring hos interessentgruppen med flere. En række af interessenter afgav et høringssvar, som er optryk i afsnit 8. Høringssvarene indgik som oplæg til konferencen.

Konference

Den 12. og 13. april 1994 vurderede et panel af lægfolk på en konference, efter konsensuskonference-modellen, forslaget om et privatkort. Panelets slutdokument er optrykt som afsnit 9.

Formidling

Der blev udsendt en pressemeddelelse om den foreløbige rapport/pjecen og forslaget om et privatkort. Forslaget om privatkort og konferencen gav anledning til betydelig omtale i aviser, tidsskrifter, radio og TV. Endvidere blev projektet formidlet på forskellige møder.

Anbefaling og slutformidling

På baggrund af udredningen og evalueringen er der udarbejdet nogle afsluttende anbefalinger, som findes i afsnit 10.

Projektet slutformidles med nærværende endelige rapport. Rapporten vil blive tilsendt Folketinget. Desuden vil den blive sendt til Indenrigsministeriet, CPR-kontoret som gennemfører et forprojekt om et elektronisk borgerkort. Dette forprojekt blev igangsat bl.a. på baggrund af Teknologinævnets projekt og forventes afsluttet august 1994. Endvidere vil rapporten blive sendt til det udvalg regeringen nedsatte i april 1994 om "Informationssamfundet år 2000", der som del af et indsatsområde nævner: "I forhold til borgerne vil udviklingen af et elektronisk borgerkort kunne betyde både forbedret service og administrativ effektivisering".

Projektets resultater vil endvidere blive formidlet til offentligheden, Europakommissionen m.fl.

[16] Hans Siggaard Jensen og Ole Skovmose: Teknologikritik - et teknologifilosofisk essay (1986). s. 100ff.
[17] Tine Hansen, Oluf Danielsen, Jørn Ravn:
Teknologivurdering i Danmark - en orientering. Teknologi Nævnet (1992). S.9.
[18] Hans Siggaard Jensen, Peter Pruzan og Ole Thyssen: Den etiske udfordring (1990). S. 74.

3. Ic-kort teknologien

Plastkort begyndte at blive anvendt som kreditkort i 50'erne i USA og spredte sig til Europa i 60'erne. Det var de internationale kreditkort kæder (f.eks. Diners Club og American Express), som var bærer af denne udvikling. Et stort teknologisk skridt var introduktionen af magnetstriben og dermed muligheden for elektronisk læsning af oplysninger på kortet i slutningen af 60'erne. Anvendelsen heraf var først udbredt i slutningen af 70'erne.

Ideen om at indbygge en programmérbar indretning i et plastkort blev skabt af franskmanden Roland Moreno i midten af 70,erne, men var på det tidspunkt ikke teknisk muligt. Umiddelbart forekommer det også temmelig håbløst, når man tænker på, at kortets tykkelse er 0,76 mm. Men i begyndelsen af 80,erne fik det sine første praktiske udformninger. Det var nu muligt at fremstille integrerede kredse, der var så små, at de kunne lægges ind i kortet.

Selv om plastkort i dag er meget udbredte må man sige, at der er tale om en ganske ny teknologi.

a) Ic-kort

Ic-kortet, der også betegnes som chip-kort, smart-kort, computerkort kan som enhver computer programmeres, og dermed udføre databehandling og har mulighed for at opbevare data.

Kommunikationen sker ved at kortet anbringes i en kortlæser (card accepting device), som via en kontakt-knap på kortet kan overføre og modtage data. Kontaktknappen har 8 kontakt-punkter til strømforsyning, klokke, dataudveksling og to friholdte punkter til senere udvikling.

En nyere udvikling af ic-kortet er det såkaldte kontaktfri kort, der i stedet for kontakt-knappen kommunikerer ved et elektromagnetisk felt eller ved radiobølger.

Det næste forsøg i udviklingen er ic-kort med indbygget display og tastatur. Det kan karakteriseres som et aktivt kort, fordi det kan fungere uden ydre enheder. Opgaven med at få et sådant kort til følge standard tykkelsen på 0,76 mm er kolossal.

I denne udredning menes med et ic-kort et kort med en kontakt-knap og kommunikation via en kortlæser.

Fysisk format

Generelt for plastkortene er der fastlagt en standard for selve kortets fysiske udformning. Standarden er fastlagt af den Internationale Standardiserings Organisation (ISO) i standarderne IS7810 og indgår i IS7816-1.

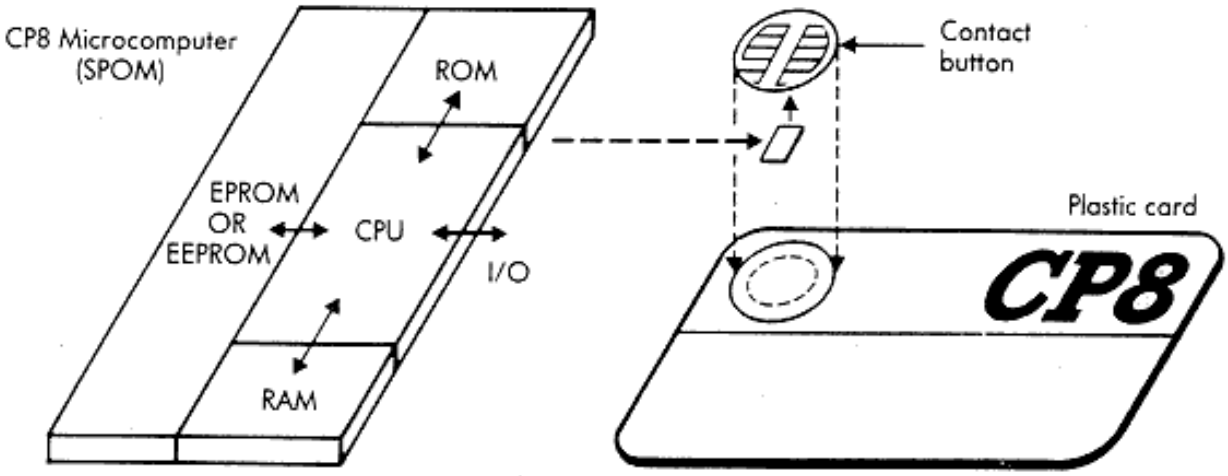
Kortet skal overholde målene 85,7 mm lang, 53,9 mm høj og en tykkelse på blot 0,76 mm.

Kontaktknappens placering er fastlagt i ISO-standarden IS7816.

Ic-kortet kan iøvrigt udformes med f.eks. fortrykte oplysninger, prægede oplysninger, stregkode, foto og felt til underskrift.

Ic-kortets computer

Bag kontakt-knappen ligger den integrerede kreds, kortets computer, der også betegnes som en SPOM (self programmable one chip microcomputer). Den integrerede kreds' størrelse er ca. 25 mm2. Den består af en CPU (central prossesing unit), computerens regneenhed, og forskellige typer lager RAM, ROM og EPROM eller EEPROM. CPU'en er en 8 bit enhed og arbejder ved 3MHz.



De tre lager typer har forskellige egenskaber og anvendelse.

RAM (random access memory) er et arbejdslager for CPU'en. Det er kendetegnet ved en hurtig access tid. Indholdet slettes når strømforsyningen ophører, dvs når kortet forlader kortlæseren. RAM lagerets størrelse er typisk 224 bytes.

ROM (read only memory). Data i ROM lageret indlægges ved kortets fremstilling og kan ikke slettes eller ændres i kortets levetid. Dataindholdet bevares uafhængig af strømforsyning, og anvendes til operativsystem, programmel til kryptering af data i kortet og visse systemdata. ROM lageret størrelse er typisk 6-10 Kbytes

EPROM/EEPROM (electrically programmable read-only memory/electrically erasable programmable read-only memory). En hukommelse, eller blivende lager, hvor data kan opbevares i perioder mellem kortets anvendelse, dvs. når der ikke er strømforsyning. Hertil benyttes programmable read-only memory (PROM), som tillader indlæsning af data. Der er to versioner af PROM: EPROM og EEPROM. Ic-kort findes i dag med en hukommmelseskapacitet på op til 64 Kbytes.

I en kommende standard 7816-4 skelnes mellem interne datafiler, som kun benyttes af kortet, og arbejdsfiler, hvis dataindhold kan kommunikeres til kortlæser og kortbruger. Til hver arbejds-datafil kan der knyttes en adgangskontrol, dvs. beskyttelse af hvornår filen kan læses.

Ic-kortet er i dag udviklet til multifunktionskort, som kan håndtere et antal forskellige anvendelser, der kan bruges uafhængigt af hinanden i forskellige miljøer. Standarden 7816-4 giver et standardiseret grundlag for sådanne kort. IBM's multifunktionskort har et ROM-lager på 10 Kbytes og et EEPROM-lager på 8 Kbytes [19] . Til et svensk sikkerhedsprojekt, "Allterminalen" har Philips leveret et multifunktionskort, som håndterer en række krypteringsnøgler og algoritmer [20] .

Hvordan et ic-kort udformes afhænger naturligvis af det system det skal indgå i. De enkelte leverandører har forskellige kort, og til større systemer kan den integrerede kreds (chippen) specialdesignes.

Standarder

Standardiseringen af ic-kortet begyndte i begyndelsen af 8o'erne i ISO. I 1990 blev der i den Europæiske standardiserings organisation (CEN) nedsat en Technical Comittee om plastkort [21]. Dansk Standard er via udvalget om identitetskort (s147u17) aktive i dette arbejde.

En lang række standardiserede krav til ic-kort med kontakt findes i ISO-standard 7816:

IS7816-1 IC-cards with contacts - physical characteristics
IS7816-2 IC-cards with contacts - dimensions and location of contacts
IS7816-3 IC-cards with contacts - electronic signals and transmission protocols
CD7816-4 IC-cards with contacts - interindustry commands for interchange

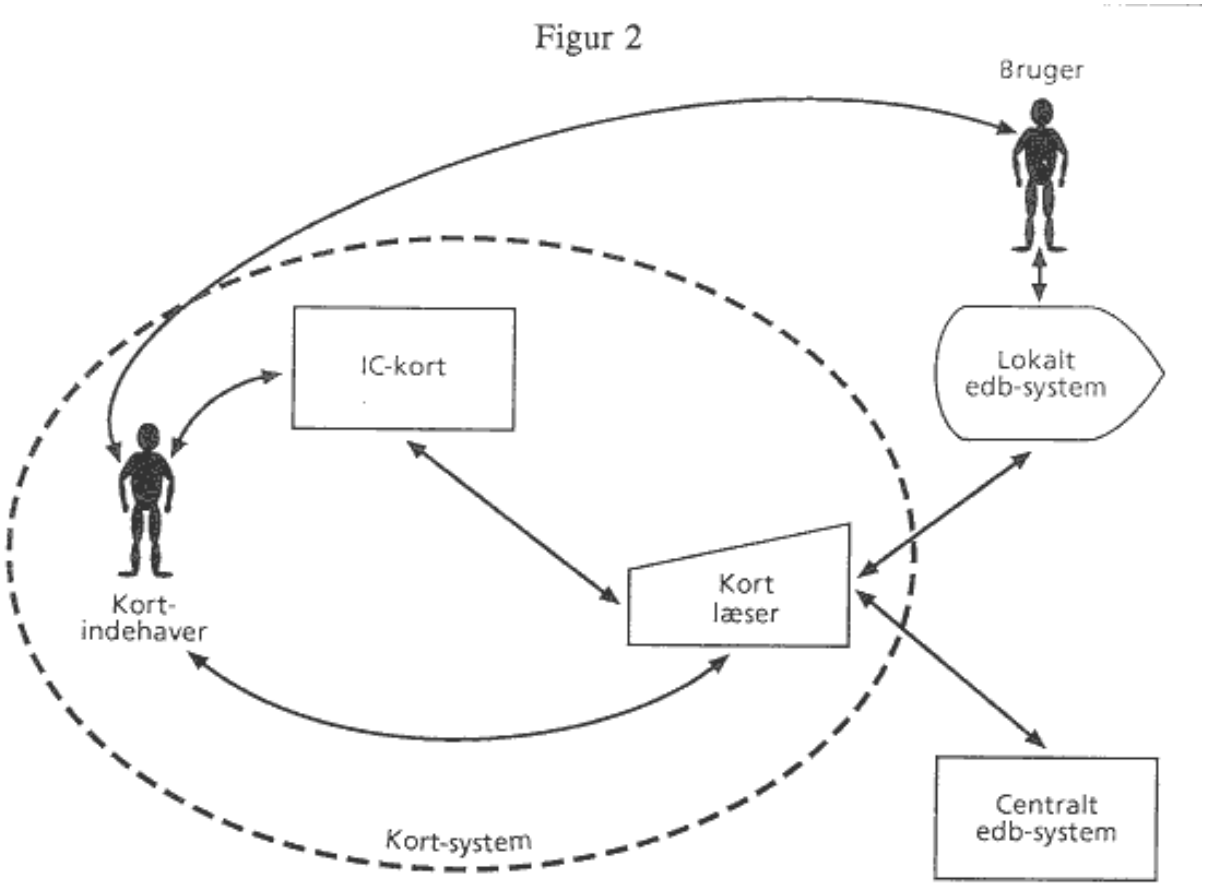
Disse ISO-standarder suppleres af CEN-standarder, der i visse tilfælde udfylder dem. F.eks. er der i CEN-standarden taget stilling til en valgmulighed for kontaktknappens placering, så denne ligger fast i Europa.

b) Kort-system

Et ic-kortet indgår altid i et samlet system, hvor ic-kortet kun er en lille del. I dette afsnit fremlægges en oversigt over sådanne systemers aktører, dvs. mennesker, organisationer og edb-systemerne, og sammenhænge mellem dem. Formålet er at fremlægge den terminologi, som anvendes i udredningen.

I figur 2 findes en systembeskrivelse over en anvendelse af kortet.

Figur 2



Overordnet har vi tre systemer:

System Med system henvises til det samlede system, hvor anvendelsen af ic-kortet indgår.

Kort-system Med kort-system henvises til den del af systemet, som direkte handler om brugen af kortet. Grænsefladen er kommunikationen mellem kort-læseren og edb-systemet. Kort-systemet er angivet med den stiplede linje.

Edb-system Med edb-system henvises til et edb-baseret system hos en organisation. Edb-systemet har en grænseflade til et kort-system, dvs. det er en del af edb-systemet, at nogle brugere (kortindehavere) benytter et ic-kort. Edb-systemet kan være et lokalt system, hvor der samtidig er en menneske-menneske dialog, eller det kan være et centralt system, hvor kortindehaveren alene er i en menneske-maskine dialog.

De enkelte aktører i systemer er:

Kort-indehaver Med kort-indehaver henvises til den person, der har et ic-kort, og som ved angivelse af en identifikation kan benytte kortet.

IC-kort Med ic-kortet henvises til et plastkort med en integreret kreds, dvs. til teknologien. Kortet omtales også med henvisning til anvendelsen, f.eks. id-kort, betalingskort eller sundhedskort. Og endelig har udstedte kort ofte et produktnavn, f.eks. Dankort, Danmønt, sygesikringskort.

Kort-læser Kortlæseren er et edb-udstyr, som kan etablere kommunikation mellem kortet og kortindehaveren og edb-systemet. Kortlæsere kan være udformet med forskellige funktioner, f.eks. til dialog med kortindehaveren eller kryptering af data før kommunikation til edb-systemet. Kort-læseren kan være uafhængig af det edb-system, den kommunikerer med, eller være knyttet til et bestemt edb-system, som det kommunikerer isoleret med.

Bruger af edb-system Med bruger henvises til personer, som arbejder med edb-systemet.

Ic-kortet kan beskrives nærmere med:

Anvendelse Med anvendelse henvises til den måde et ic-kortet anvendes på i et system.

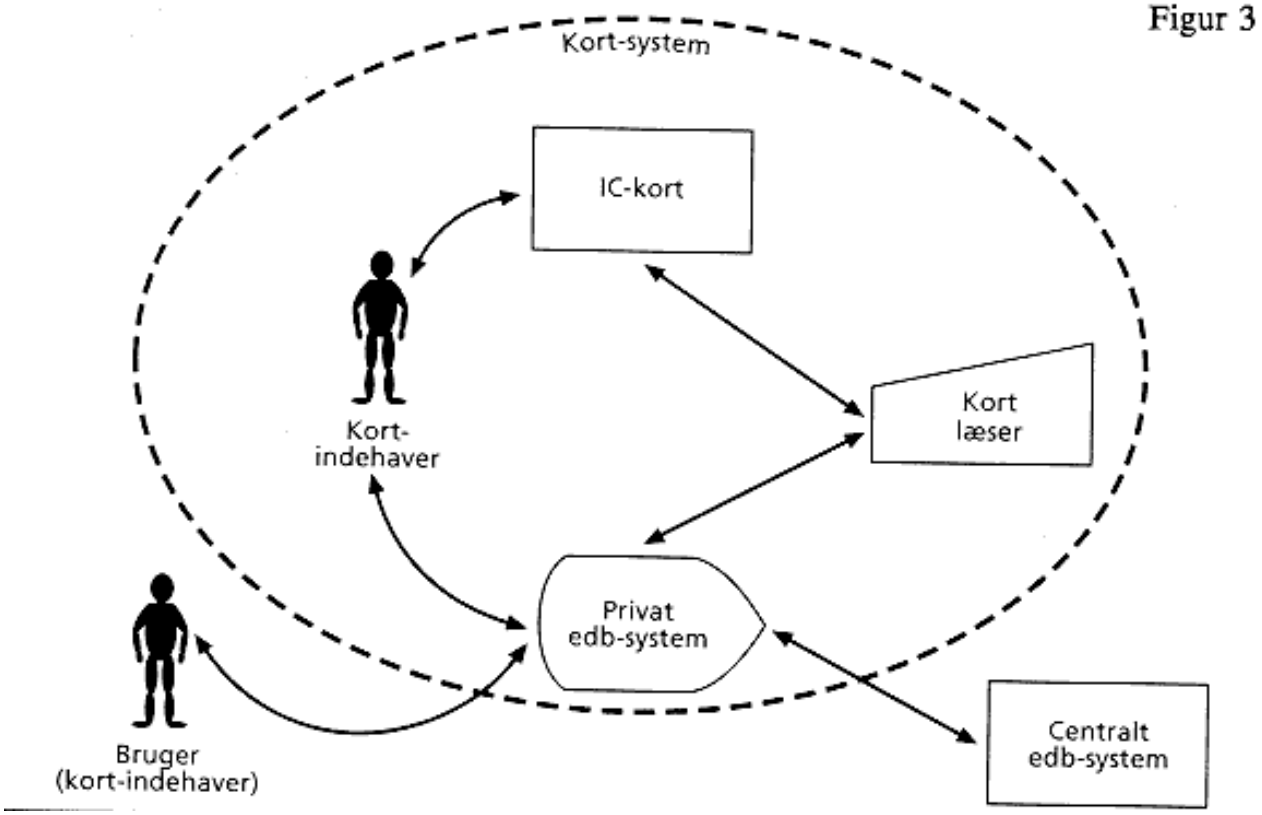
Kort-funktion Med en kort-funktion henvises til en elektronisk databehandling kortet kan udføre. Der er tale om en logisk funktion, og ikke en beskrivelse af løsningen i kortet.

Tjeneste Med tjeneste henvises til programmer og data i kortet som benyttes til en (eller flere) kortfunktioner.

Pilene illustrerer kommunikation mellem elementerne. Kommunikation mellem edb-maskiner er selvfølgelig en elektronisk datakommunikation, mens kommunikation mellem mennesker typisk er mundtligt. Kommunikation mellem menneske og edb-maskiner er fysisk, f.eks. indlæsning af kort, indtastning og udskrift af oplysninger.

I figur 3 vises en systembeskrivelse af et lidt andet system. Kortindehaveren benytter kortet sammen med et privat edb-system, typisk på egen pc i hjemmet. Kortindehaveren optræder her også i rollen som bruger.

Figur 3



Men der er flere aktører i systemet. For at vise dem er systemet beskrevet fra en organisatorisk synsvinkel i figur 4.

De nye aktører som ses her er:

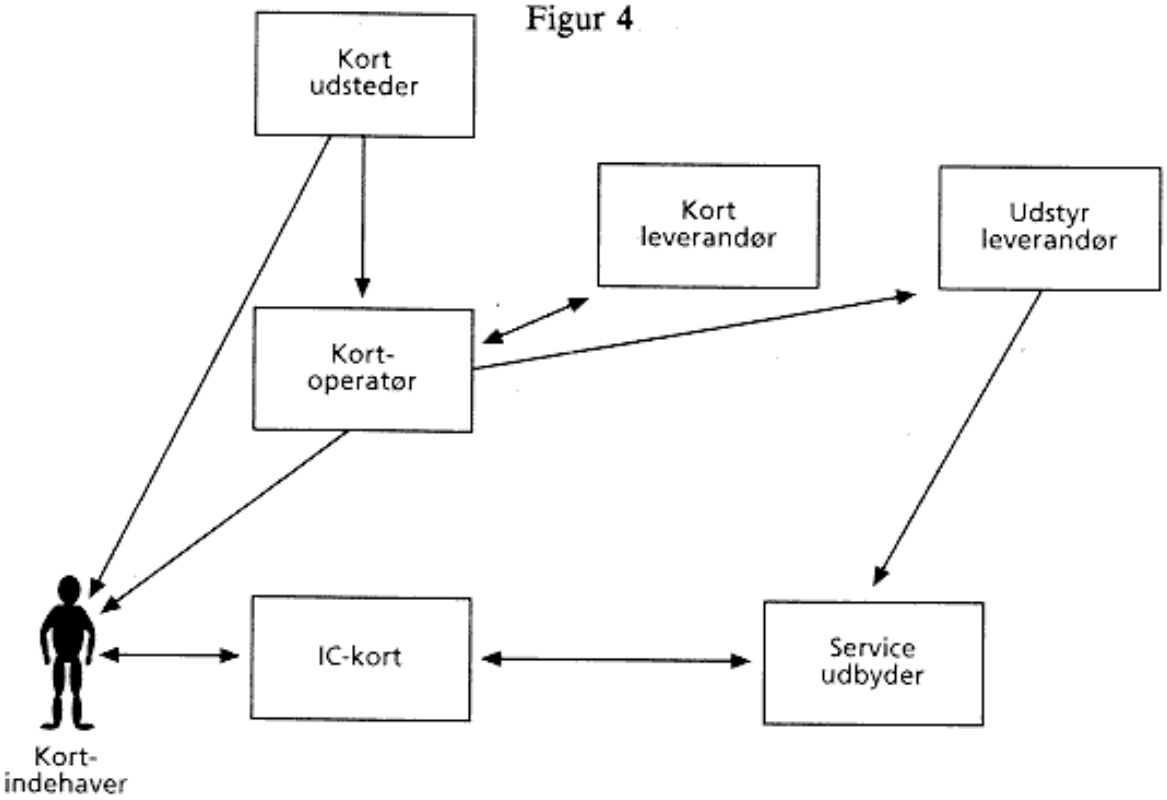
Kort-udsteder Med kort-udsteder henvises til den organisation (offentlig myndighed eller privat virksomhed), som er juridisk ansvarlig for udstedelse af kortet og kort-systemets drift og sikkerhed.

Kort-operatør Med kort-operatør henvises til den organisation, som er teknisk ansvarlig for udlevering af kort, kort-systemets drift og sikkerhed. Kort-operatøren kan være identisk med kort-udsteder, men kan også være en anden organisation, der udfører opgaven i et kontraktforhold.

Service-udbyder Med service-udbyder henvises til den organisation, som er ansvarlig for driften af et edb-system, som ic-kortet kan indgå i.

Kort-leverandør Med kort-leverandør henvises til de virksomheder som producerer ic-kortet.

Figur 4



Udstyrleverandør Med udstyrleverandør henvises til de virksomheder som leverer udstyr og programmel (f.eks. kort-læsere) til kort-systemet.

Pilene illustrerer relationer mellem aktørerne. Kort-udsteder er ansvarlig for kort-operatørens virke. Kort-operatøren definerer bl.a. standarder m.v., som leverandørerne skal følge, og gennemfører evt. godkendelsesafprøvning. Og kort-udsteder køber kort hos kort-leverandørerne. Kort-operatøren fastlægger også standarder, som service-udbydere skal anvende for at kunne inddrage kort-anvendelsen i deres edb-system. Kort-operatør udleverer kortet og overvåger kortenes anvendelse, herunder behandling af mistede kort. For nogle anvendelser skal service-udbyderen godkendes af kortudsteder og etableres i kort-systemet. Service-udbydere køber udstyr af udstyrsleverandørerne. Kort-udsteder udgiver vejledning og retningslinjer for kort-indehaveren bl.a. om brug af kortet og beskyttelse af identifikationen (pin-kode eller lignende).

Standarder

I de internationale standardiseringsorganisationer arbejdes der på at standardisere en række anvendelser. I CEN (den europæiske organisation) er der nedsat arbejdsgrupper (under TC224) om:

- tværsektorielle anvendelser, hvor man bl.a. arbejder med et generelt koncept, herunder PIN-koder og sikkerhed,
- telekommunikationsanvendelser, hvor man bl.a. arbejder med betalings-specifikation, anvendelse til betalings-telefoner, anvendelse i GSM-telefoner,
- specifikation for finansielle transaktioner, herunder standard for en elektronisk pung,
- transport anvendelser, bl.a. fly-billetter
- sundhedskort med administrative og/eller medicinske data
- betalings-TV,
- uddannelse,
- access-kontrol [22].

Endnu foreligger der ikke færdige standarder for anvendelser af ic-kortet.

Begrundelsen for at benytte standarderne er, at man kan indkøbe kort, udstyr og programmel som er almindelige, dvs. billigere, og at kortet har en mulighed for at blive anvendt i andre sammenhænge. Udstedelse af et multifunktionskort, som skal kunne fungere i et åbent system, forudsætter, at kortet og anvendelserne kan gennemføres på grundlag af standarder. Det skal nævnes, at der findes standarder for en række sikkerheds-spørgsmål, f.eks. bruger autenticitet, og for krypterings-teknikker og deres anvendelser.

[19] IBM: IBM Multi Funktion Card. General Information (1993)
[20] Smart Card News December 1993.
[21] Henning N . Jensen: Chip-kort standardiseringen er ved at komme igang. IT-Standardnyt februar 1991.
Alain Cohen-Aloro: Standardisering af IC-kort - fortid, nutid og fremtid. IT-standardnyt oktober 1992.
[22] Alain Cohen-Aldoro: Standardisering af IC-kort - fortid, nutid og fremtid. IT-Standardnyt oktober 1992

4. Anvendelses-eksempler

Afsnittet rummer analyser af en række eksempler på anvendelser af et borger ic-kort. Eksemplerne belyser mulige kort-funktioner, også nogle, som der ikke findes konkret planer om at gennemføre. Formålet med eksemplerne er at give et bredt grundlag for debat om eventuelle borger ic-kort, og analysen holder sig derfor på et overordnet plan.

Analysen af eksemplerne er foretaget som en forandringsanalyse [23].

Forandringsanalysen er en arbejdsopgave som gennemføres før man tager beslutning om forandringer. Den er ikke en forstudie-fase i et systemudviklingsprojekt, men "bör vara och ses som ett separat steg och avslutas med en beslutspunkt" (s. 11). En forandringsanalyse opstartes på grundlag af forskellige opfattelser af eksisterende problemer, her: skal vi have et borger ic-kort?. I en proces veksles mellem at afdække problemer, fastlægge mål og opstille forandringsforslag, så man går fra vage og ukendte problemstillinger og mål til en mere fælles opfattelse. Forandringsanalysen kan slutte med tre resultater: ingen forandring, bestemte forandringer eller afvikling.

4.A Bruger-identifikation

Når en person starter en elektronisk kommunikation med et edb-system er det nødvendigt, at personen kan identificere sig overfor edb-systemet på en sikker måde. Egentlig skal edb-systemet også identificere sig over for personen, men det ser vi bort fra her. Denne bruger-identifikation er nødvendig for edb-systemets adgangskontrol, dvs. kontrol af at brugeren har ret til at benytte systemet.

I dette afsnit behandles tre anvendelses-eksempler:

a) Pinkoder og betalingskort
b) Adgang til kommunal egenservice
c) Adgangskontrol til edb-system

a) Pinkoder og betalingskort

Borger ic-kortet kan erstatte bruger-identifikationen ved eksisterende betalingskort og dermed også betalingskortet. For at det kan lade sig gøre skal ic-kortet opbevare betalingskortets data (kontonummer mv.) og kort-indehaverens pin-kode.

Mål

* Pin-koder og betalingskort kan erstattes af borger ic-kortet
* Kort-indehaveren kan dokumentere anvendelse af "betalingskortet"
* Mulighed for fælles konto og pin-kode inden for familien

Beskrivelse

I stedet for de nuværende betalingskort, f.eks. Dankortet, anvendes borger ic-kortet. Kortet anbringes i terminalen/kortlæseren og efter at kort-indehaveren har identificeret sig, vælger han den service-udbyder som betalingskortet skal bruges overfor, f.eks. en bank, forretning, konto-kæde. Herefter er proceduren den samme som i dag.

Borger ic-kortet skal kunne anvendes de steder, hvor man i dag anvender betalingskort elektronisk, f.eks. kontantautomater og terminaler i forretninger.

De opbevarede pin-koder er beskyttet på kortet, så de ikke kan læses af uvedkommende og kun kan frigives til anvendelse efter kortindehaverens identifikation. Kortindehaveren behøver derfor ikke at huske pin-koden til de forskellige betalingskort, men kan principielt nøjes med at huske en kode til borger ic-kortet.

Da borger ic-kortet - i modsætning til eksisterende betalingskort med magnetstribe - har såvel databehandlings- som lagerkapacitet kan der dannes en log-fil over udførte betalingstransaktioner. Log-filen kan indeholde et vist antal transaktioner, f.eks. de sidste 99. Opstår der tvivlsspørgsmål om en betaling eller ønskes der en oversigt kan log-filen udskrives af kort-indehaveren.

På borger ic-kortet kan pin-koder mv. indlægges og slettes løbende ved anvendelse af særlige procedurer. Der er derfor mulighed for, at man i en familie kan dele konti og koder som led i den fælles økonomi.

Vurdering

Alle betalingskort, som har en kortindehaveridentifikation, anvender en firecifret pin-kode til verifikation af, om den der vil bruge betalingskortet faktisk er kort-indehaveren.

Mængden af koder man skal anvende og huske ser ud til at stige. Ud over betalingskortene anvendes pin-koder f.eks. til videoudlejnings-kort, audiotexsystemer via telefonen, opkald via hjemmecomputer til databaser, adgangskontrol på arbejdet. Man kan næppe huske mere end en eller to pin-koder, som anvendes jævnligt, og man er derfor nødt til at skrive resten ned.

En gruppe borgere af talblinde, evnesvage, demente m.fl. kan ikke huske tal-koder og afskæres fra at anvende en i stigende grad central teknologi. Hvis der til borger ic-kortet anvendes en biokode, f.eks. fingeraftryk eller venemønster, til kortindehaveridentifikation vil det bidrage til at mindske problemet for denne gruppe.

Det er erkendt, at det er et problem for den enkelte at huske pin-koderne. I forbindelse med Dankortet har pengeinstitutterne udviklet en PIN-KODE HUSKER, der er en farvepalet, hvor pin-koden kan skjules, men huskes på farvekombinationen. På posthusene udbydes et såkaldt "SecretCard", der kan opbevare 10 pin-koder, som kan aflæses ved at oplyse én pin-kode.

Problematikken omkring pin-koder har ført til særlige ansvarsregler i lov om betalingskort.

Pin-koder til bruger-identifikation udgør et problem, som med øget udbredelse af elektronisk kommunikation må forudses at blive betydeligt. Hvis det ikke er muligt at holde pin-koderne hemmeligt udgør det en alvorlig sikkerheds-trussel, der giver risiko for misbrug.

Muligheden for at dele konti og pin-kode må vurderes som en forbedring af forbrugerens situation.

Idag har kort-indehaveren reelt ingen muligheder for at bevise, at han ikke har anvendt sit betalingskort. Og da domstolene accepterer et systembevis må man konstatere, at kort-indehaverens retstilling er dårlig [24] . Det må vurderes som en væsentlig forbedring af kort-indehaverens retstilling, hvis transaktionerne registreres i en log-fil.

Det må sammenfattende vurderes, at der her er en oplagt kortfunktion i borger ic-kortet. Men det skal bemærkes at konsekvensen er, at der over en periode skal foretages en udskiftning af udstyr og ændringer af edb-systemer.

b) Adgang til kommunal egenservice

I dette anvendelses-eksempel benyttes borger ic-kortet til bruger-identifikation overfor et kommunalt egenservicesystem (elektronisk selvbetjening).

Mål

* Borgerne skal have mulighed for en sikker identifikation ved selvbetjening og adgang til egne personoplysninger i kommunens edb-registre
* Den kommunale forvaltning får mulighed for at etablere egenservice på områder, hvor det ellers ikke er muligt

Beskrivelse

Ideen i egen-service systemerne er, at borgeren/kunden kan kalde op til et edb-system og selv udføre forskellige "forretninger" [25]. Egen-service systemer findes som rene informations-systemer, hvor man ringer op med telefonen og via en menu kan komme frem til bestemte typer oplysninger som bliver læst op. I dag udbygger pengeinstitutterne deres egen-servicesystemer, så kunden med telefonen kan gennemføre forskellige bankforretninger f.eks. overførsel af beløb fra en konto til en anden. Systemer der anvender telefonen er tale-systemer, dvs. det svar man får, bliver læst op af en indtalt stemme.

Tale-systemer er anvendelige til informations-systemer og enkle interaktive opgaver. Men til mere komplekse eller omfattende systemer er de ikke brugbare. Sådanne egen-servicesystemer forudsætter, at brugerne har en terminal - f.eks. en speciel type (en minitel) eller en pc med kommunikations-program og modem - som anvendes til kommunikationen med systemet. Informationerne kan læses på skærmen, og der kan gives forskellige kommandoer, som i et almindeligt edb-program. Et koncept kaldes for video-tex og det bygger på en enkel brugergrænseflade, der gør det let at anvende.

Der har været gennemført forsøg i Suså og Ballerup kommuner med videotex-systemer. I Ballerup blev der opstillet 22 videotex terminaler på offentlige steder: biblioteker, posthuse, rådhuset, ungdomsklubben, pensionist-centeret og boligselskaber. I Suså har 80 familier fået terminalen hjem, og 8 terminaler er opstillet på biblioteket, kommunekontoret samt nogle skoler.

Systemerne har hovedsagelig været informations-systemer. Dernæst har systemerne haft en postkasse eller opslagstavle, hvor brugeren kunne skrive til en anden person eller en gruppe personer. Endelig har man i Ballerup kunnet skrive sig på en venteliste til boliger, og i Suså var der koblet en række private erhvervsdrivende på, hvor man f.eks. kunne bestille varer. I Ballerup var der, over en periode på 11 måneder, godt 30.000 opkald, hvilket svarer til 169 opkald pr. terminal pr. måned. I Suså var der, over en periode på 8 måneder, små 2.000 opkald, hvilket svarer til 38 opkald pr. terminal pr. måned. I forhold til franske erfaringer er denne brug af systemerne meget høj. Den kan dog skyldes nyhedens interesse. (AKF-Nyt s. 24-25).

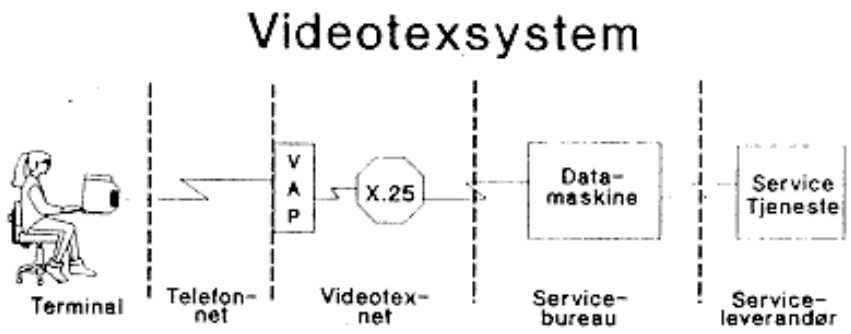
I rapporten om forsøg med egenservice vurderes, at "i fremtiden må man dog forestille sig mange slags edb-systemer som dele af egenservice. Ren information kan være én del, andre dele kan være: Bestilling og afbestilling af hjemmehjælp, skatteberegning, pensionsberegning, ekspertsystemer om miljøforhold, udløsning af ejendomsskatter fra lønkontoen, fejlmelding af gadebelysningen, reservation af bøger på biblioteket, brevkasser til "levende" eksperter, og meget, meget andet" (Egenservice s. 22).

Jydsk Telefon og Kommunedata m.fl. arbejder i et fælles selskab, Diatel, på at kunne udbyde et videotex-system i 1994. Man regner her med at kunne markedsføre en særlig kommunepakke, der kan indgå i systemets tilbud af private og offentlige servicer.

Egen-service i kommunen udelukker ikke, at borgeren henvender sig på rådhuset og bliver betjent, men kan ses som et tilbud. "For mange mennesker er det en lettelse i en travl hverdag ikke at være afhængig af rådhusets åbningstid, og for andre har det givet mulighed for at forberede sig før kontakt med de ansatte i kommunen". (AKF-nyt s. 25)

Terminalerne som giver adgang til systemet kan tænkes opstillet på offentlige steder, f.eks. rådhuset, biblioteket eller banegården, men det optimale er, at de kommer ud i hjemmene. "Offentligt opstillede skærme er ikke udelukkede, men hvis de er eneste mulighed for egenservice, vil de begrænse udbuddet af kommunale services og gøre selvbetjeningen mindre effektiv, end den kunne være" (Egenservice s. 39). Man kan tænke sig særlige terminaler (minitelapparater som kendes fra Frankrig og blev uddelt i Suså kommune), eller terminaler sammenbygget med telefonen (der findes smart-telephones der også har en skærm, og vi kender sammenbyggede fax/telefon), eller hjemmets pc'er kan anvendes (opgørelser viser, at 24% af alle hjem i 1992 havde en pc'er).

Et videotex system kan teknisk beskrives således:



Fra: Egenservice

Det er teknisk muligt, at kommunen overdrager en lang række opgaver til borgeren. Men skal borgeren f.eks. have adgang til kommunens edb-registre for at give supplerende oplysninger eller have indsigt i registrene, og skal borgerens oplysninger danne grundlag for sagsbehandling (evt. automatiseret) forudsætter det, at der sker en sikker identifikation. I de kendte systemer hos pengeinstitutterne anvendes en pin-kode (et fire-cifret tal).

Vurdering

Det er næppe realistisk eller sikkert at udstyre alle borgere med en kommunal pinkode?

Har borgerne et borger ic-kort er der derimod mulighed for at opbygge det kommunale egen-service system med en sikker identifikation. Terminalerne udbygges med en kortlæser og dermed kan der etableres en sikker identifikation.

Denne bruger-identifikation kan praktisk tilrettelægges på forskellige måde. Et eksempel: Borgeren kalder op til systemet og sætter sit borger ic-kort i kortlæseren. Her identificerer borgeren sig over for kortet. Terminalen kan herefter give meddelelse til egen-servicesystemet om kortnummer og kort-indehaverens cpr-nr. Egenservicesystemet kan herefter kontrollere i et centralt register (f.eks. CPR), at kortnummer og cpr-nr. hører sammen. Efter denne sikre identifikation kan man åbne for en række interaktive funktioner (registerindsigt, ændringer af indtægtsgrundlag ved boligsikring, ændring af venteliste til daginstitution osv.).

En anden fremgangsmåde kan tilrettelægges ved at anvende et krypterings-nøglepar (se nærmere herom i afsnit 4.B og 4.C), så egenservicesystemet sender en tilfældig tekst-streng til borger ic-kortet, som krypterer tekst-strenge og personens cpr-nummer med den private nøgle. Denne krypterede værdi sendes til egenservice systemet sammen med et certifikat med den offentlige nøgle. Ved at dekrypterede denne værdi kan egenservicesystemet dels verificere brugeridentifikation og dels få oplyst cpr-nummer.

Således vil et borger ic-kort være en løsning på en sikker bruger-identifikation over for en kommunes egenservice. Den sikre identifikation vil give mulighed for at tilbyde egenservice, som rækker langt ud over den rene information fra kommune til borger.

Det skal bemærkes at der ikke i beskrivelsen ovenfor er behandlet en række andre relevante sikkerheds-spørgsmål.

c) Adgangskontrol til edb-system

I dette anvendelses-eksempel benyttes borger ic-kortet til adgangskontrol til et edb-system.

Mål

* Den enkelte får mulighed for en mere sikker adgangskontrol til personlige edb-systemer
* Mere sikre pc-baserede systemer og dermed et mere robust samfund

Beskrivelse

Adgangskontrollen til edb-systemer kan bygge på fire metoder:

- Hvad en person *ved*, f.eks. et kendeord (password)
- Hvad en person *har*, f.eks. et kort
- Hvad en person *er*, f.eks. et fingeraftryk
- Hvad en person *har lært*, f.eks. en beregning eller en underskrift.

Ved mange pc-baserede systemer, specielt i private hjem, anvendes ingen adgangskontrol. Når der findes en adgangskontrol, er den første metode den mest almindelige. Brugeren oplyser et kendeord på 6-8 karakterer (bogstaver, tal og specialtegn). De andre metoder findes, men har en beskeden udbredelse, og kun i erhvervsmæssige systemer.

Ved at benytte en særlig krypterings-teknik med et såkaldt nøglepar kan der med borger ic-kortet etableres en meget sikker adgangskontrol til edb-systemer på en pc [26]. (Kryptering er omtalt i afsnit 4.B og C) Adgangskontrollen bygger på at et særligt

sikkerheds edb-program på pc'en kender kortindehaverens offentlige nøgle og kan kontrollere, at borger ic-kortet sidder i en kort-læser mens pc'en anvendes. Når man ønsker at benytte pc'en anbringes borger ic-kortet i en kortlæser og kortindehaver identifikationen gennemføres. Herefter gennemføres en dialog mellem pc'ens sikkerhedsprogram og kortet, som verificerer om pågældende har ret til at benytte systemet.

Vurdering

I dag er pc'er meget svage i sikkerhedsmæssig henseende. Anvendelse af kendeord er på mange måder problematisk og giver ikke en høj grad af sikkerhed. Med den meget hastige udbredelse af pc i samfundet, såvel i erhvervsliv som privat, er den manglende sikkerhed et samfundsproblem. En styrkelse af pc-sikkerheden vil bidrage til et mere robust samfund i forhold til anvendelse af elektronisk informations-teknologi.

Det må vurderes, at et borger ic-kort vil kunne bidrage væsentligt til øge sikkerheden ved pc'ere.

4.B Digital signatur

I dette anvendelses-eksempel bruges et borger ic-kort til at opbevare nøgler til at danne en digital underskrift.

Mål

* Den enkelte har mulighed for at afgive en bindende elektronisk underskrift

Baggrund

Elektronisk kommunikation bevæger sig hastigt fra at være noget store organisationer beskæftiger sig med til at blive en del af hverdagen for de fleste borgere. I det næste ti-år vil kommunikation mellem borgerne, mellem borgeren og offentlige myndigheder og mellem forbrugeren og private virksomheder i stigende grad kunne ske elektronisk og efterhånden blive en naturlig del af hverdagen.

De tekniske forudsætninger for denne udvikling er skabt. Gennem standardisering af åbne systemer med grundlag i reference-rammen OSI (Open Systems Interconnection) fra begyndelsen af 1980'erne er der etableret muligheder for åben kommunikation nationalt og internationalt. Standarder for en række datakommunikations-tjenester er vedtaget eller på vej. Dernæst er man ved at gennemføre en total digitalisering af de offentlige datanet. Pc'ere markedsføres i højere grad som medier til kommunikation i forhold til tidligere som maskiner til databehandling.

Elektronisk post er en åben kommunikation, som må forventes at få stor udbredelse. Der er vedtaget en international standard, X.400. Den danske udgave markedsføres med betegnelsen "Datapost 400" (Datapost400) [27]. I det elektroniske post-system sendes "brevet" med angivelse af modtager-adresse fra sin pc'er til post-systemet. X.400 arbejder efter et såkaldt "store-and-forward" princip, dvs man modtager brevet og opbevarer det indtil modtageren henter det i sin postkasse. Gennem den fælles standard er det muligt at sende e-post til mere end 30 udenlandske X.400 systemer. Datapost ser selv store perspektiver: "X.400 er det fuldelektroniske svar på det mange hundrede år gamle traditionelle postsystem. /../ Som system betragtet vil X.400 være det redskab som på længere sigt vil kunne bevise rationaliseringsgevinsten ved indførelse af informationsteknologien ikke kun i den offentlige forvaltning, men i hele samfundet i bredeste forstand."(s. 8) Den elektroniske post vil kunne anvendes i kommunikation mellem borgere (i Danmark og globalt), til kommunikation med offentlige myndigheder og i kommunikation med private virksomheder og organisationer.

Homebanking, homeshopping, egenservice hos kommunen er eksempler på en udvikling henimod, at borgerne privat kan gennemføre forskellige "forretninger". Der anvendes i dag ofte trykknap-telefonen som teknologi, men systemer, der er skærmbaserede (enten med særlige videotekst-skærme eller pc-baserede) er på vej.

Et andet felt, hvor kommunikation i åbne net hurtigt udvikler sig, er dokument-udveksling (EDI, Electronic DataInterchange). Med EDI tænkes på overførsler af data, der er struktureret i overensstemmelse med en fastlagt standard, fra datamaskine til datamaskine. Ordrer og fakturaer vil blive kommunikeret direkte til modtagerens edb-system, som umiddelbart kan arbejde videre med oplysningerne og f.eks. iværksætte en vareleverance [28]. Der kan etableres standarder for forbrugerkøb, således at man afsender en indkøbsordre struktureret på en given måde, som umiddelbart kan behandles af virksomhedens edb-system.

Problem

Denne udvikling står sikkert over for en række forskelligartede problemer. Her skal fremhæves, at der ikke er etableret en brevtroværdighed, der kan sikre,

- at brevet kommer uændret frem til den rigtige (integritet),

- at modtageren har vished for, at brevet er fra den angivne afsender (autenticitet) og - at afsenderen ikke bagefter kan nægte, at have sendt brevet (uafviselighed) [29].

"Tidligere blev dette problem løst ved originale dokumenter, som til en vis grad er uforfalskelige. Informationen er skrevet på en sådan måde, at det er svært at tilføje eller slette tekst (information) uden at efterlade spor, og en håndskreven underskrift bekræfter rigtigheden /../ Hvordan sikrer man så ægtheden af elektroniske dokumenter?" (Landrock s. 176)

Man kan *ikke* forestille sig, at der kan indgås bindende aftaler uden brevtroværdighed og underskrift, eller foretages indkøb og betalingsformidling uden vished for, at bestilleren rent faktisk er den han udgiver sig for, eller åbne for, at der foretages bankforretninger ud over uden sikkerhed for, at de afgivne ordrer til banken kommer fra den rigtige person og ikke bagefter kan benægtes. Hvis der ikke findes en almindelig tilgængelig løsning for brevtroværdighen kan man ikke forestille sig, at den elektroniske kommunikation kan få nogen særlig udbredelse.

Problemet er erkendt

Telestyrelsen nedsatte i oktober 1991 en arbejdsgruppe, som har arbejdet med myndighedskrav på krypteringsområdet og her specielt overvejet regulering af såkaldte nøglecentre. Den afsluttende rapport blev færdig juni 1993 [30].

De danske pengeinstitutter har i PBS opbygget et system til digital underskrift, TeleSec [31]. Systemet er på vej til at blive indført af pengeinstitutterne. Det forventes at TeleSec efterhånden vil blive en sikkerhedsstandard i kommunikationen mellem bankerne og deres kunder, primært erhvervskunder. Efter PBS' opfattelse vil systemet også kunne anvendes i andre brancher end bankvæsen.

Inden for rammerne af EU's INFOSEC program arbejdes der med en række projekter om elektronisk underskrift [32].

Løsningen er også kendt

Løsningen er at underskrive de elektroniske dokumenter med en elektronisk underskrift. En elektronisk underskrift kan dannes ved anvendelse af en krypterings-teknik, der kaldes for public key. Denne fremgangsmåde kaldes for digital underskrift og er fastlagt i en international standard (IS9796). Kryptering betyder generelt forvanskning af data på en kontrolleret måde så de senere kan genskabes. (Se nærmere herom i tillæg i afsnit 4.C). Public key kryptering bygger på, at der findes to nøgler: en offentlig nøgle, som alle har adgang til, og en privat og hemmelig nøgle, som kun opbevares hos pågældende nøgle-indehaver (evt. hos en betroet tredjepart). Nøglerne har den egenskab, at når en tekst er krypteret med den ene, kan den kun bringes tilbage til sin oprindelige form med den anden. Den digitale underskrift etableres netop ved, at man krypterer en tekst med den private nøgle, da teksten kun kan genskabes med den tilhørende offentlige nøgle er det entydigt fastslået, at den kommer fra indehaveren af den private nøgle, og dermed er underskriften etableret. Normalt krypterer man ikke hele teksten men en såkaldt hashværdi for teksten, dvs. et tal der er beregnet ud fra teksten. Dermed sikrer man at teksten ikke er blevet ændret. Hvis man så endelig tilføjer hashværdien dato og tidspunkt og krypterer disse data med den private nøgle kan afsenderen ikke senere nægte at have sendt brevet på et bestemt tidspunkt. Det vil kunne dokumenteres, at teksten ikke er ændret, at den er sendt af en bestemt person, og vedkommende kan ikke "løbe fra det". Dermed har man opnået den samlede brevtroværdighed, og brevet er underskrevet.

Beskrivelse

Den mest udbredte fremgangsmåde for et public key system er RSA opkaldt efter dens tre fædre: Rivest, Shamir og Adlemann. Nøglerne er store tal på 200 cifre, så de kan ikke huskes eller indtastes, men må opbevares og overføres elektronisk. Ic-kortet er meget velegnet til at opbevare disse nøgler. På kortet kan opbevares såvel den offentlige nøgle som den private nøgle. Den private nøgle opbevares kun i personens kort, og med sådanne sikkerhedsforanstaltninger, at den udelukkende er tilgængelig for kort-indehaveren.

Ethvert system til elektronisk underskrift kræver, at der oprettes et nøglecenter - omtalt som Certificate Authority eller Trusted Third Party. Nøglecenterets opgaver er bl.a.

- at sikre nøglernes kvalitet
- at opbevare identiteten mellem den offentlige nøgle og indehaveren
- at udstede certifikater, dvs. bekræfte identiteten for en given offentlig nøgle
- at udlevere den offentlige nøgle, dvs. fungere som "telefonbog".

Når to danskere har et borger ic-kort, som indeholder deres krypterings-nøgler (den offentlige og den private hemmelige) vil en brevudveksling med digital signatur kunne forløbe således: [33]

- Det dokument der ønskes sendt elektronisk udfærdiges.
Der kan være tale om et brev skrevet på et almindeligt tekstbehandlings-system, eller et dokument redigeret i overensstemmelse med en EDI-standard, eller en transaktion lavet på (en særlig) telefon eller skærm, eller noget helt fjerde.
- Når dokumentet er færdigt, aktiveres et særligt edb-program, som laver en digital underskrift.
Efter navngivning af dokumentet bliver den underskrivende bedt om at placere sit ic-kort i en kort-læser og gennemføre kortindehaver-identifikationen. Der dannes nu en digital underskrift på ca. 100 bogstaver, som er entydigt knyttet til teksten. Underskriften føjes til dokumentet på en separat side sammen med den underskrivendes identitet og evt. den offentlige nøgle.
- Dokument kan nu afsendes til modtageren, som normalt vil bekræfte modtagelsen. Ved modtagelse af dokumentet kan den elektroniske underskrift kontrolleres ved anvendelse af den medsendte offentlige nøgle. Har modtageren ikke tidligere fået nøglen verificeret hos nøglecenteret må der ske en henvendelse hertil for at få en bekræftelse på, at den oplyste offentlige nøgle hører til vedkommende afsender. Herefter kan nøgle og identitet opbevares til senere brug, svarende til en registrering af navn og telefonnummer.

CCITT standarden X.509 [34] beskriver en fremgangsmåde, hvor nøglecenteret udfærdiger et særlig certifikat, som indeholder den offentlige nøgle og er forsynet med nøglecenterets digitale underskrift. Certifikatet kan sendes med det underskrevne dokument og modtageren behøver kun at opbevare nøglecenterets offentlige nøgle for at kunne kontrollere underskriften på alle breve.

Afviger dokumentet den mindste smule fra originaldokumentet, som var grundlag for den elektroniske underskrift, vil uoverensstemmelsen blive opdaget ved kontrollen af den digitale underskrift. Dokumentet vil herefter ikke kunne anvendes.

Lagrer modtageren dokumentet elektronisk vil, man senere kunne gentage kontrollen af dokumentet - og f.eks. bevise, at man har modtaget pågældende dokument fra afsenderen.

Rent praktisk udføres den digitale signatur og kontrol af en modtaget signatur at et edb-system, som kan anvendes uden kendskab til de tekniske og matematiske finesser der ligger bag fremgangsmåden.

Vurdering

Det er nødvendigt at indføre en digital underskrift, hvis man vil udbygge anvendelsen af åbne systemer og åben kommunikation, hvor deltagerne i kommunikationen ikke på forhånd behøver at kende hinanden. I modsat fald vil systemet vil blive tilrettelagt, som lukkede systemer hvor service-udbyderne har registreret kunderne og etablerer egne sikkerhedsforanstaltninger f.eks. PIN-koder.

Muligheden for at kunne danne en digital underskrift kan siges at være en del af infrastrukturen i den åbne datakommunikation - lige som standarder for åbne systemer og datanettet er det. Elektronisk datakommunikation må antages at få stor betydning for den enkelte borger - og for offentlige myndigheders og private virksomheders rationaliserings-bestræbelser.

Det kan samlet vurderes at en kort-funktion, der kan danne en digital signatur er meget relevant for et borger ic-kort.

4.C Brevhemmelighed

I dette anvendelses-eksempel anvendes borger ic-kortet til at sikre, at breve og anden post, som sendes elektronisk, kan krypteres.

Mål

* Den enkelte får mulighed for at sikre at breve, dokumenter o.l. ikke kan læses af uvedkommende

Beskrivelse

Det må forventes, at anvendelse af elektronisk post og anden elektronisk kommunikation vil blive en del af hverdagen (se afsnittet "baggrund" ovenfor i 4.B). Lige som der ikke for øjeblikket tilbydes en generel løsning for brevtroværdigheden, tilbydes der heller ikke en generel løsning til sikring af brevhemmeligheden.

Det elektroniske brev kan tænkes opsnappet under data-transmissionen, eller det kan blive hentet af uvedkommende i modtagerens postkasse, hvor flere kan have adgang eller en person skaffer sig uberettiget adgang. Det elektroniske brev kan blive dirigeret videre til et lokalnet eller en pc, hvor flere har adgang til brevet. I dag må man betragte elektronisk post som en åben forsendelse, svarende til teksten på et postkort.

Udover disse konkrete problemer med brevhemmeligheden kan man sige, at det principielt bør være muligt, at sende sin post fortroligt. Valget af om det i den konkrete situation er nødvendigt må være den enkeltes, og bør ikke være en afgørelse som er taget ved tilrettelæggelse af systemet.

Teknikken til at sikre brevhemmeligheden er kryptering af brevindholdet. Krypteringen indebærer at dataene forvanskes på en måde så de kun kan læses af den, der har en bestemt nøgle (se nærmere om kryptering i tillægget nedenfor).

Krypteringen kan f.eks. udføres på følgende to måder.

1) Brevet kan krypteres med modtagerens offentlige nøgle i public-key nøgleparret. Herefter er det kun indehaveren af den private nøgle, som kan genskabe teksten. Det kunne være en enkel måde i kommunikation af kortere breve, f.eks. mellem to privatpersoner. Normalt anses metoden dog for upraktisk, fordi kryptering med RSA-algoritmen er tidskrævende.
2) Brevet kan krypteres med DES-algoritmen, som anvender samme nøgle til kryptering og dekryptering. Denne kryptering er meget hurtig. Problemet med denne metode er, at den anvendte nøgle skal udveksles på en sikker måde, fordi brevhemmeligheden er gået tabt, hvis andre får adgang til nøglen. Problemet kan løses ved at danne en tilfældig nøgle, som kun anvendes til et enkelt brev. Denne nøgle sendes med brevet, krypteret med modtagerens offentlige public-key nøgle.

I praksis udføres kryptering mv. af et program, der en del af brugerens edb-system. Brugeren skal derfor blot sætte funktionen igang.

Det skal bemærkes at fremgangsmåden også kan benyttes til at kryptere data på sin egen pc. I stedet for at sende de krypterede data, lagres de på pc'ens harddisk eller en diskette. Nøglen til DES-krypteringen kan lagres sammen med dataene krypteret med brugerens offentlige nøgle. En anden mulighed er, at der på borger ic-kortet opbevares en DES-nøgle, som anvendes til kryptering af egne data.

Vurdering

Et ic-kort er meget velegnet til at opbevare forskellige krypterings-nøgler, og det vil dermed være muligt med et borger-kort at tilvejebringe en generel løsning på brevhemmelighed ved elektronisk post.

Muligheden for enhver til at sikre brevhemmeligheden for sin egen post kan, lige som brevfortroligheden med en digital signatur, siges at være en del af infrastrukturen i den åbne datakommunikation.

Tillæg: kryptering

Anvendelse af krypterings-teknikker er et grundlæggende værktøj ved de fleste sikkerhedsforanstaltninger ved datakommunikation i åbne net [35].

I ordbogen forklares kryptering med hemmelig skrift. Det drejer sig om at gøre en *klartekst* ulæselig for uvedkommende. Klarteksten *krypteres* ved anvendelse af en *krypterings-algoritme* (en fremgangsmåde), der er styret af en *nøgle*. Nøglen styrer, hvordan man (datamaskinen) anvender krypterings-algoritmen til at regne og flytte rundt på delene (bogstaver eller bits) i

klarteksten. Den ulæselige tekst kaldes for *chiffertekst*, og hensigten er, at klarteksten kan genskabes ved *dekryptering* af chifferteksten ved hjælp af nøglen. På den anden side kan klarteksten ikke genskabes når man ikke har adgang til nøglen [36].

Historisk er kryptering knyttet til militær og diplomati. Faktisk var det en af datamaskinens første opgaver at bryde fjendens krypterings-algoritme under 2. verdenskrig. En helt banal krypterings-algoritme er kendt som Cæsars chiffer. Hver bogstav udskiftes (algoritmen) med bogstavet tre pladser før (nøglen) i alfabetet. Mere avancerede substitutionsmetoder blev udviklet før datamaskinens indtog. En kendt metode er Vigenére chiffer, hvor nøglen er en bogstavsstreng, som oftest bestod af gentagelse af samme ord. Algoritmen er fortsat at bogstavet udskiftes med et andet bogstav, men antallet af pladser er bestemt af bogstavet i nøglen, f.eks.: et A betød 0 pladser og et E betød 4 pladser.

Klartekst:	Kryptering
nøgle:	teknologinævn
chiffertekst:	avflepcros

Selvom teksten "avflepcros" ser temmelig ulæselig ud er krypteringen svag overfor en systematisk kryptoanalyse, bl.a. fordi nøglen gentages.

Man anvender i dag typisk to krypterings-algoritmer. DES kaldes for en symmetrisk eller enkelt-nøgle metode, da man anvender samme nøgle til kryptering og dekryptering. RSA kaldes for en asymmetrisk eller public-key (offentlig-nøgle) metode, da man har to nøgler - hvor den ene er offentlig tilgængelig og den anden privat/hemmelig - der hver især kan kryptere og dekryptere en chiffertekst krypteret med den anden nøgle.

DES

DES, der står for Data Encryption Standard, er udviklet af IBM og har været amerikansk standard. DES kryptering er meget anvendt og kan implementeres som programmel eller i en selvstændig chip. DES anvendes f.eks. mellem Dankort-terminalerne og PBS.

DES bygger på, at man udskifter "bogstaver" med et andet og supplerer med at flytte rundt på dem.

Grundlaget for elektronisk kryptering er XOR funktionen:

klartekst	1 XOR nøgle	0 = 1	i chifferteksten
	1 XOR	1 = 0	
	0 XOR	0 = 0	
	0 XOR	1 = 1	

Det særlige man udnytter er at gennemføres operationen baglæns, altså chiffertekst XOR nøgle genskabes klarteksten. Man gennemfører en såkaldt substitution på bit-niveau. Substitutionen kombineres med en såkaldt transposition, dvs. ombytning af en bitstreng fra klarteksten med en anden bitstreng.

I DES består nøglen af 64 bit, hvoraf de 8 er paritetbits. Der kan således dannes 2^{56} forskellige krypteringsnøgler.

I algoritmen arbejdes med blokke af 64 bit. Først foretages en initial permutation af de 64 bit, der skal krypteres. Dvs. de blandes. Herefter opdeles de 64 bit i to dele á 32 bit - en venstre og en højre side. Gennem 16 iterationer substitueres de enkelte bit ved anvendelse af XOR og mellem hver iteration bytter de to halvdele side. Tilsidst gennemføres den inverse permutation. Hele krypteringen styres af den valgte nøgle på en kompleks, men fuldstændig beskrevet måde. Dekryptering sker ved at gennemføre processen baglæns.

DES algoritmen er offentlig tilgængelig for enhver, som vil sætte sig ind i alle detaljer. Ligeledes er det muligt at se programmer som udfører krypteringen. Det er en pointe ved kryptering, at styrken ikke ligger i at hemmeligholde hvordan man gør, men at måden man gør det på giver tilstrækkelig sikkerhed.

Public key (RSA)

Public Key systemer bygger på at der findes to nøgler - en offentlig og en privat hemmelig. Den mest udbredte algoritme er RSA opkaldt efter dens tre fædre: Rivest, Shamir og Adlemann.

RSA algoritmen anvender modulus n aritmetik. En blok af klarteksten opfattes som et tal. Krypteringer sker ved beregningen K^e

mod n (hvor K=en blok af klarteksten, e og n udgør krypteringsnøglen). Klarteksten kan genskabes ved beregningen C^d mod n (hvor C=samme blok af chifferteksten, d og n udgør krypteringsnøglen). d og e har den egenskab, at man også kan gennemføre krypteringen omvendt. Men man kan ikke genskabe klarteksten ved at anvende samme nøgle.

Udgangspunktet for at finde nøglerne er at bestemme en værdi for n, der skal være produktet af to primtal (p og q), der begge er på mindst hundrede cifre. n er således et tal på ca. 200 cifre. Hver bruger har sit eget "n". Dernæst vælges et tal e som skal være relativ primisk med (p-1)(q-1), dvs. ikke har nogen fælles faktorer med p-1 eller q-1. Med kendskab til p og q er det så muligt at beregne d.

En meddelelse der er krypteret med den private nøgle kan genskabes af enhver ved anvendelse af den offentlige og alment tilgængelige nøgle, men det er dokumenteret, at meddelelsen er afsendt af indehaveren af den hemmelige nøgle. Public Key systemet er som skabt til at danne en digital underskrift og sikre brevtroværdighed, fordi kryptering med den private nøgle entydig knytter dokumentet til nøglens indehaver.

Hvis en meddelelse er krypteret med modtagerens offentlige nøgle, kan den kun de-krypteres af indehaveren af den private nøgle. Det betyder, at man kan sikre en brevhemmelighed, dvs. at dokumentet ikke kan læses af andre end modtageren. Principperne i RSA-krypteringen er illustreret i tegneserien.

I forbindelse med elektronisk underskrift anvendes normalt en hashfunktion, som er et tal, der beregnes ud fra dokumentet, men er væsentlig mindre. Til dette tal knyttes en tidsangivelse, der herefter krypteres med afsenderens private nøgle. Da hashfunktionen værdi er entydig i forhold til et givent dokument (men ikke omvendt), dokumenterer det, at dokumentet er sendt af en bestemt bruger og ikke er ændret.

Konceptet med digital signatur, kryptering og et offentligt og privat/hemmeligt nøglepar (public key og secret key) kan være svært at forstå. Vi bringer derfor igen kærlighedshistorien om Alice og Bob, som Lene Sekjær har tegnet efter oplæg fra Peter Landrock. Bob og Alice er meget forelskede i hinanden. Men Bob er rejst til udlandet for at arbejde, og nu kan han ikke holde det ud mere. Han savner Alice og vil giftes med hende. Men i baggrunden lurer en dunkel skikkelse fra Bobs fortid...

Historien om Alice og Bob

Alice sidder i Danmark...

...og Bob i et andet EF-land. De har hver sin terminal og krypteringsudstyr.

Bob skriver et glødende kærlighedsbrev og sender det til Alice. Brevet er krypteret med Alices offentlige nøgle.

Alice modtager brevet, som hun håber, er fra Bob og dekrypterer det med sin egen hemmelige nøgle.

Dorrit har lyttet med på linien, men kan ikke dekryptere kærlighedsbrevet (hun elsker også Bob!).

Alice er i tvivl. Er brevet virkelig fra Bob? Enhver kunne have sendt den krypterede besked - alle kender Alices offentlige nøgle!

Så Alice ringer til Bob...

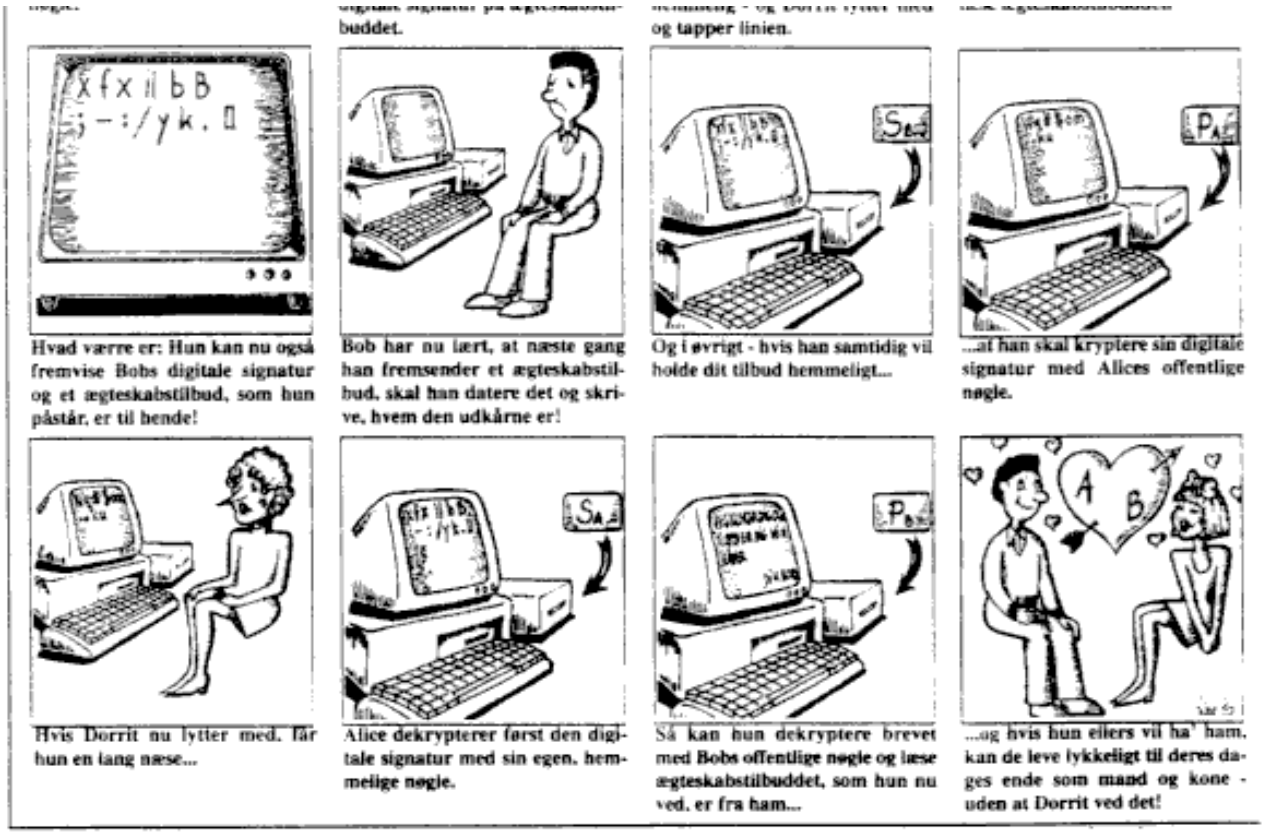
Bob elsker virkelig Alice, så han krypterer brevet igen, nu med sin egen, hemmelige nøgle...

...og Alice dekrypterer med bankende hjerte - og Bobs offentlige nøgle.

Nu har hun vished, og bordet fanger for Bob. Han har jo sat sin digitale signatur på meddelelsen.

Men en fare truer den unge lykke: Forlovelsen skulle have været hemmelig - og Dorrit lytter med

Hun kender jo også Bobs offentlige nøgle og kan dekryptere og læse meddelelsen.



4.D Registerkontrol

Borgerkort har en tæt sammenhæng med offentlige myndigheders edb-registre med personlige oplysninger. I dette afsnit belyses borger ic-kortets muligheder for at borgerne får mere kontrol med de oplysninger, der registreres i registrene.

I dette afsnit behandles tre anvendelses-eksempler

a) Hemmeligholdelse af egne personoplysninger (sagsbehandling)
b) Samtykke til videregivelse (kvikskranke)
c) Elektronisk egenadgang til edb-registre

a) Hemmeligholdelse af egne personoplysninger (sagsbehandling)

I dette anvendelses-eksempel behandles muligheder for, at klienten kan hemmeligholde personlige oplysninger i en socialsag.[37]

Mål

* Borgeren sikres fuld hemmeligholdelse af visse typer oplysninger i en sag

* Sagsbehandleren sikres fortrolighed i sagsbehandlingen

* Tillidsforholdet mellem klient og sagsbehandler afspejles i data-behandlingen

Baggrund

I sagsbehandling af en socialsag indhentes en række oplysninger. Den primære kilde er naturligvis borgeren selv, men der suppleres med fortrolige eller rent private oplysninger fra andre registre. De oplysninger, som samles i sagsbeskrivelsen er dels hvad man kan kalde objektive fakta - som kan være mere eller mindre følsomme - dels en række "bløde" og mere subjektive oplysninger (f.eks. om alkoholforbrug/misbrug, mulig skilsmisse, børns tyveri osv.). Den sociale sag kan indeholde mange oplysninger, som giver grundlag for en helhedsvurdering. Blandt oplysningerne kan også være forhold, som ikke bliver endelig belyst, men som pågældende sagsbehandler gerne vil have med. Blandt denne type oplysninger findes ofte meget følsomme rent private forhold. Et eksempel er en revalideringsansøgning, hvor ansøgeren har en kriminel fortid. Her vil nærmere oplysninger om årsagen være af betydning for erhvervsvalg, men oplysningerne vedrører iøvrigt ikke andre. Et andet eksempel er helbredsoplysninger - f.eks. oplysning om at vedkommende er HIV positiv - som personen måske tilbageholder af frygt for, at de kommer ud til andre. En oplysning om at personen er homoseksuel kan være relevant i sagen, men i øvrigt helt ligegyldig.

Borgeren (klienten) har ofte afgivet sådanne oplysninger i en slags fortrolighed med pågældende sagsbehandler - ikke som en generel oplysning til kommunens sagsjournal eller register.

I kommunerne er der en naturlig udvikling i gang i henimod, at den enkelte sagsbehandler gennemfører hele sagsbehandlingen, dvs. skrivearbejde, journalarbejde, registrering i SA-systemet og udbetaling. Den fuldførte sagsbehandling betyder: færre fejl, kortere sagsbehandlingstid og større jobtilfredshed [38] betyder også, at den sagsbehandler, som har modtaget de personlige oplysninger fra borgeren, også er den eneste som skal se dem.

Problem: hemmeligholdelsen utilstrækkelig

Uanset de nuværende regler i registerlov m.v. om behandling af personlige oplysninger kan hemmeligholdelse af de nævnte bløde/subjektive oplysninger opleves utilstrækkelig af såvel borgeren, som den sagsbehandler der skriver dem. Oplysninger af denne karakter vil utvivlsomt kunne mistolkes og/eller misbruges i andre sammenhænge. En ny sagsbehandler vil måske læse dem anderledes, eller de kan indgå i en anden sag.

Løsning: kryptering af visse oplysninger

I forbindelse med en sagsbehandling kan der ske en udskillelse af personlige oplysninger, som kun skal være tilgængelig med personens tilladelse og normalt som led i en personlig samtale/sagsbehandling, når vedkommende er til stede. Hvilke data afgøres af borgeren og sagsbehandler i en dialog.

Når sagsbehandlingen er afsluttet, og der er truffet en afgørelse, enten mens borgeren er til stede eller i umiddelbar tilknytning hertil, bliver de følsomme oplysninger krypteret. Dvs. de bliver gjort ulæselige, medmindre man har en nøgle, som kan bringe den krypterede tekst tilbage til den oprindelige form. Krypteringen sker på grundlag af en nøgle som borgeren har med på sit borger ic-kort. Kortet anbringes i en kortlæser og efter en identifikation af kortindehaver frigiver borgeren sin nøgle. De krypterede data kan ikke læses af nogen. Først når borgeren er til stede og har sin nøgle med på kortet, kan dataene igen gøres læselige.

Løsningen bygger på, at borgerne på deres borger ic-kort har et nøglepar: en offentlig og en privat nøgle der har den egenskab, at de hver især kan anvendes til kryptering af en tekst, men at kun den anden kan bringe den krypterede tekst (chifferteksten) tilbage til klartekst. Krypteringen af sagsteksten sker med den offentlige nøgle. Den kan forvaltningen få fra borgerens kort og frit opbevare i sagen (den er jo offentlig) eller den kan elektronisk hentes fra et "Nøglecenter". Teksten kan kun bringes tilbage til klarteksten med borgerens private nøgle, og den findes kun tilgængelig på borgerens kort.

Det system som opbevarer sagsjournalen skal kunne sikre, at oplysningerne ikke læses af andre, mens den foreligger i klartekst (og at der ikke tages backup, uden at teksten krypteres forinden.

Vurdering

Muligheder for at styrke borgernes kontrol med de meget følsomme oplysninger bør udnyttes og fortroligheden mellem sagsbehandler og borger er et princip, der sættes højt i sociale sager. Et borger ic-kort med et public-key nøglepar giver på en enkel måde mulighed for at styrke borgernes kontrol med meget følsomme data i kommunens edb-registre.

b) Samtykke til videregivelse (kvikskranke)

I dette anvendelses-eksempel behandles muligheden for at borger ic-kortet anvendes til at give samtykke til videregivelse af personoplysninger fra edb-registre til brug for en sagsbehandling i en kommunal kvikskranke.

Mål

* Mulighed for at udbygge sagsbehandlingsområder i kvikskranker

* Borgernes data i forskellige registre kan genbruges uden at det krænker den personlige integritet

Beskrivelse

En del kommuner (i 1990 ca. 30) [39] oprettet kvikskranker (under et eller andet navn). "Kvikskrankerne er karakteriseret ved at varetage en del af flere forvaltningers borgerrelaterede opgaver. Kvikskrankemedarbejderne har kompetence til at træffe afgørelser og færdigbehandle en række af de lettere sagsbehandlinger" (s. 7). Kvikskrankerne er oprettet ud fra ønsker om at øge servicen over for borgerne, at modernisere den kommunale organisation og at effektivisere de kommunale ressourcer (s. 8). I kvikskranken kan borgeren få løst en lang række sager, som f.eks. batterier til høreapparater, boligtilskud, buskort til pensionister, børnefamilieydelser, folkeregisteropgaver, tilskud til efterskole, knallertbevis, lettere skattesager, udbetaling af personlige tillæg (s. 17).

Problem: samtykke til videregivelse

For at løse en række af disse opgaver må medarbejderne i kvikskranken have adgang til kommunens edb-systemer. Det har rejst problemer om autorisation af adgang til personoplysninger i kommunens forskellige registre. Der kan være tale om skatteoplysninger (indtægtsforhold), oplysning om boligsikring- og tilskud, oplysninger fra en socialsag.

Ifølge register loven kan der ikke umiddelbart hentes oplysninger i forskellige edb-registre til en sagsbehandling. Som udgangspunkt skal der foreligge et samtykke fra borgeren. Det er begrundet med, at personoplysningerne skal anvendes til det formål, som de er indhentet hos borgeren til, og at vedkommende skal have kontrol med evt. udlevering og anden anvendelse. Registertilsynet har bl.a. udtalt om kvikskranken, at det er en "klar forudsætning, at den enkelte medarbejder alene autoriseres til de dele af edb-registrene, som er nødvendige for dennes arbejdsopgaver. Registertilsynet forudsætter endvidere, at sagsbehandlingen i rådhusbutikkerne tilrettelægges således, at det sikres, at sagsbehandlingen hviler på en forudgående henvendelse fra borgeren, og at borgeren i de tilfælde, hvor det som led i sagsbehandlingen kan være nødvendigt at indhente oplysninger fra forskellige forvaltningsgrene, er indforstået hermed." (Cirkulæreskrivelse af 8.10.90)

Det kunne være ønskeligt på samme tid, på den side at sikre borgeren kontrol med videregivelse af oplysninger fra edb-registre, og på den anden side at give mulighed for en bredere adgang til videregivelse for at undgå, at de samme oplysninger skal indhentes flere gange.

Løsning: samtykke med kort

En løsning er, at de edb-systemer som skal afgive registrerede oplysninger kræver at borgeren har givet sit samtykke (sin tilladelse) og at det rent fysisk er sket ved at pågældendes borger ic-kort er til stede, og at der er afgivet en meddelelse til systemet. I denne dialog kan det sikres, at borgeren får lejlighed til at angive, hvilke oplysninger der må videregives (sendes fra systemet til sagsbehandleren).

Identifikationen sker ved, at borger ic-kortet anbringes i en kortlæser og borgeren identificerer sig over for kortet. Herefter spørger terminalen om der kan ske videregivelse og borgeren giver sin accept efter en nærmere præcisering af, hvad der kan videregives. Først efter denne dialog kan medarbejderen få udleveret oplysninger fra edb-registeret.

Hvis henvendelsen sker telefonisk kan man i en fremtid, hvor borgerne har pc'er eller lignende med en kortlæser, forestille sig, at dette elektroniske samtykke bliver sendt over telefonnettet til medarbejderen. Proceduren er uændret, idet borgeren blot anvender en terminal i sit eget hjem.

Vurdering

Ved at benytte borger ic-kortet til elektronisk samtykke åbnes der mulighed for, at man kan hente personoplysninger fra forskellige registre. Samtidig kan borger ic-kortet give borgeren en større kontrol med denne videregivelse af oplysninger.

På baggrund af eksemplet med kvikskranken kan det vurderes, at denne kort-funktion kan benyttes i andre situationer, hvor man har brug for at indhente oplysninger fra forskellige edb-registre til en konkret sagsbehandling.

c) Elektronisk egen adgang til edb-registre

I dette anvendelses-eksempel giver borger ic-kortet adgang til egne personoplysninger i offentlige myndigheders edb-registre.

Mål

* Borgerne får adgang til oplysninger om sig selv i de offentlige registre

* Borgernes kontrol med egne personoplysninger styrkes

Beskrivelse

Retten til at få oplyst, hvad der er registreret om en selv i edb-registrene betragtes som en nødvendig del af en persondatabeskyttelse. Der er således registerindsigt til såvel private som offentlige edb-registre, med visse undtagelser.

I praksis anvendes denne ret til registerindsigt i meget begrænset omfang. Årsagen hertil diskuteres, men det er nærliggende at pege på praktiske vanskeligheder og manglende information til befolkningen om retten til registerindsigt.

Registerindsigten giver mulighed for at få oplyst hvilke oplysninger der er registreret. Man får således ikke information om oplysningerne er blevet anvendt. "Der er grund til at overveje, hvorvidt indsigtsretten har et tilstrækkeligt omfang i og med, at der kun kan opnås oplysninger om indholdet i de enkelte registre, men derimod ikke om, hvorvidt de registrerede oplysninger er blevet videregivet eller samkørt" (Blume s. 212).

I en rapport fra Teknologinævnet foreslås at "Et naturligt næste skridt bør være, at den enkelte borger med en høj grad af sikkerhed får elektronisk adgang til egne persondata i offentlige og private registre".

I en rapport fra Kommunedata oplyses, at en undersøgelse blandt borgerne viste at knap 40% forventede, at et kommunalt egenservice-system vil give mulighed for indsigt om sig selv i kommunens registre [42].

Vurdering

Med et borger ic-kort kan der tilvejebringes den fornødne sikre brugeridentifikation, så det offentlige, med en høj grad af sikkerhed mod misbrug, kan give borgerne adgang til egne oplysninger i edb-registrene.

Da edb-registre oprettet til forskellige formål principielt bør holdes adskilte, kan der ikke etableres en samlet indgang for borgerne til alle offentlige registre. Man vil fortsat være nødsaget til at kontakte de forskellige myndigheder. Man kunne tænke sig en offentlig database med oplysninger om, hvilke registre der findes og information om, hvordan man kan få registerindsigt til dem.

For fortrolige og rent private oplysninger skal den ansvarlige for et edb-register gennemføre en logning, dvs. registrering af, hvad oplysninger i registeret er blevet anvendt til. En elektronisk registerindsigt bør omfatte adgang til denne log-fil, så man kan se hvordan oplysningerne er blevet anvendt.

4.E Personlig legitimation

Et borger ic-kort forbindes typisk med et identitets-kort. I den danske standard, DS2341: "Identitetskort. Opbygning og informationsindhold", defineres identitetskort som "Et kort, der anvendes til personlig legitimation, og dermed forbinder en persons fysiske identitet med den juridiske identitet. Den juridiske identitet er en legitimation, der alene godtgør en persons identitet over for omverdenen."

I afsnit 4.A blev et borger ic-kort anvendt til bruger-identifikation ved elektronisk kommunikation behandlet. Det er vigtigt at skelne mellem denne anvendelse og anvendelsen til personlig legitimation. I bruger-identifikationen anvendes borger ic-kortet til at afklare (verificere) at pågældende har ret til benytte edb-systemet på bestemte måder. I den personlige legitimation anvendes

borger ic-kortet til at dokumentere (verificere), hvem personen er.

I dette afsnit behandles to anvendelses-eksempler:

a) Personlig legitimation
b) Fysisk adgangskontrol

a) Personlig legitimation

I dette anvendelses-eksempel behandles, hvordan et borger ic-kort kan benyttes til personlig legitimation og dermed fungere som et id-kort.

Mål

* Etablere en sikker og generel personlig legitimation, som kan anvendes i alle situationer, hvor der er et legitimt behov

Beskrivelse

I Danmark har vi ikke et generelt identitets-kort, som staten har udstedt til alle, og som det kræves, at borgerne altid bærer på sig og kan fremvise ved krav fra en myndighedsperson. Der findes ingen forslag om et sådant dansk identitets-kort.

I en række sammenhænge har vi behov for at legitimere os. Det kan være over for myndighederne, på posthuset, i banken osv. Her anvender vi forskellige beviser vi har modtaget: pas, kørekort, sygesikringsbevis. Disse beviser er ikke udstedt som id-kort, men som dokumentation for bestemte rettigheder. I de situationer, hvor man har behov for at legitimere sig, ville det være enklere og mere sikkert med et generelt id-kort.

Et borger ic-kort kan anvendes til personlig legitimation. For det første til en manuel/visuel dokumentation på samme måde som de nævnte beviser ved at man ser på kortet. For det andet kan et borger ic-kort anvendes til en automatisk legitimation ved at kortet anbringes i en kort-læser, og personen gennemfører en korrekt kort-indehaver identifikation.

I standarden DS2341 indeholder id-kortet følgende elementer:

- dokumentnavn
- kortudsteder
- logo
- underskrift
- kortløbenummer
- kortindehaverens navn
- personnummer eller fødselsdato
- fotografi
- dato.

For at kortet kan anvendes til manuel legitimation, må en række af disse elementer være synlige på kortet: foto, navn, underskrift.

I den automatiske legitimation udnyttes den sikre kortindehaver-identifikation, som borger ic-kortet nødvendigvis har. Det kortindehaveren beviser er, at det er vedkommendes borger ic-kort, ved at foretage en korrekt identifikation. Dermed skabes en meget stor sikkerhed, for, at det er kortindehaveren som er tilstede. I den automatiske legitimation er det muligt at foretage en kommunikation med centrale registre, f.eks. kriminalregisteret. Denne mulighed er tænkt anvendt i Schiphol Lufthavnen, hvor rejsende fra EU-lande tilbydes hurtig passage ved at anvende et særligt ic-kort. Ved kontrollen er det tanken, at der skal ske opslag i det særlige Schengen-register over eftersøgte personer.

Vurdering

Et borger ic-kort vil være et effektivt id-kort til personlig legitimation. Hvordan det anvendes kan ikke fastlægges ved kortets udformning, men er et spørgsmål om regulering ved lovgivning eller på anden måde.

Borger ic-kortet må siges at være et langt bedre id-kort end de eksisterende offentlige beviser, der idag anvendes. Et borger ic-kort vil derfor give den enkelte en mere sikker personlig legitimation og dermed også større sikkerhed for, at andre ikke kan give sig ud for én.

b) Fysisk adgangskontrol

I dette anvendelses-eksempel beskrives anvendelse af borger ic-kortet til personlig legitimation ved adgang til bygninger o.l.

Mål

- * Etablere en sikker fysisk adgangskontrol til steder hvor, en sådan kræves

Beskrivelse

Borger ic-kortet giver mulighed for en meget sikker personlig legitimation, som kan udføres manuelt eller automatisk. Et sådant id-kort kan anvendes til fysisk adgangskontrol, dvs. kontrol af, om en person må bevæge sig ind i bygning, lokale eller lignende.

Idag anvendes fysisk adgangskontrol over for medarbejdere i virksomheder mv. Her anvendes forskellige plastkort: tekstkort, magnetstribekort og ic-kort.

Man kan forestille sig en fremtid, hvor man vil gennemføre en fysisk adgangskontrol ved offentlige installationer, f.eks. lufthavne, jernbanestationer, særlige byområder, fodboldstadioner osv. for at forebygge terroristaktioner og almindelig uro. Med borger ic-kort vil sådanne kontroller kunne automatiseres og dermed gøres praktisk mulige.

Vurdering

Borger ic-kortet er teknisk set en praktisk - og når det er udstedt - billig løsning på krav om fysisk adgangskontrol.

Spørgsmålet er i hvilken udstrækning det skal tillades at anvende borger ic-kortet til fysisk adgangskontrol, f.eks. til arbejdspladser, ved offentlige lokaliteter osv.

4.F Databærer af personlige oplysninger

Anvendelse af borger ic-kort til bærer af personlige oplysninger er et forslag, der næsten altid fremføres når borger ic-kort omtales. Internationalt findes en lang række projekter, hvor ic-kort bl.a. anvendes til databærer af helbredsoplysninger. På den anden side kan det konstateres, at myndighederne i Danmark ikke viser disse muligheder særlig interesse. Det almindelige synspunkt er, at den udviklede danske infrastruktur til datakommunikation og eksistensen af et sammenhængende social- og sundhedsvæsen og en række centrale edb-registre betyder, at der ikke er noget behov for et ic-kort som databærer.

Generelt kan man opdele de data, der opbevares i tre grupper:

- *enkeltstående oplysninger*. F.eks. hastehelbredsoplysninger (blodtype, sygdomme som allergier og sukkersyge, organdonortilsagn), beviser (kørekort, jagttegn), skatteoplysninger (fradrag, trækprocent),
- *tidsbegrænsede oplysninger* som er knyttet til et sagsforløb. F.eks. journal ved indlæggelse på hospital eller ved ambulant behandling, oplysninger ved ledighedsperioder til brug i A-kasse og Arbejdsformidling, recept til apotek, oplysninger fra forskellige myndigheder, som skal bruges i en konkret sag,
- *vedvarende oplysninger* (databank). F.eks. helbredsoplysninger, socialoplysninger.

Et centralt spørgsmål når personlige oplysninger skal bæres på et ic-kort er, om dataene flyttes fra centrale edb-registre og derfor kan siges at mindske registreringen i samfundet eller om dataene kopieres på kortet med henblik på, at de så kan medtages flere steder.

For at få et bredt indtryk af mulighederne for at anvende borger ic-kort til databærer er behandlet følgende anvendelses-eksempler

a) Stamdata
b) Personlige beviser
c) Generel helbredsjournal

d) Specialiseret helbredsjournal
e) Vandrejournal i sundhedssektoren
f) Recepter/medicinforbrug
g) Nød-/advarselsoplysninger
h) Arbejdsløses sagsjournal
i) Arbejdsløses vandrejournal
j) Uddannelsesdata

Eksemplerne er udarbejdet på grundlag af regler for arbejdsformidling og A-kasser [43] og kontakt til AF-Roskilde, en lokal SID-afdeling, og litteraturstudier [44] og kontakt til personer inden for sundhedssektoren.

a) Stamdata

I dette anvendelses-eksempel anvendes borger ic-kortet til at opbevare navn, adresse og cpr-nummer på kortindehaveren og evt. på dennes mindreårige børn.

Mål

* Mulighed for maskinel overførsel af stamdata

* Mulighed for at opbevare stamdata på egne børn

Beskrivelse

På borger ic-kortet kan kort-indehaverens stamdata opbevares, f.eks. navn, adresse og cpr-nummer. Disse oplysninger kan ændres, f.eks. ved adresseændring, uden at der skal udleveres et nyt kort.

Det vil også være muligt at opbevare stamdata for egne mindreårige børn. Med mindreårige tænkes på børn der ikke har fået eget borger ic-kort. Man kan tænke sig at borger ic-kortet udleveres ved det fyldte 16. år, som sygesikringsbeviset, eller måske allerede ved 14. år.

Den væsentligste begrundelse for at opbevare stamdataene er at de så kan overføres elektronisk. I f.eks. sundhedssektoren kan der være behov for at få oplyst børns navne mv. og det kan derfor være praktisk, at de findes på borger ic-kortet og kan overføres elektronisk.

Muligheden for at overføre stamdata elektronisk må siges at være hovedbegrundelsen for at skifte papirsygesikrings-beviset ud med det nye plastsygesikringsbevis med magnetstribe.

Vurdering

Der er tale om en enkel kort-funktion, som kan etableres på et borger ic-kort.

b) Personlige beviser

I dette anvendelses-eksempel opbevares personlige beviser udstedt af offentlige myndigheder på borger ic-kortet.

Mål

* Opbevaring af personlige beviser med henblik på en sikker dokumentation og opnåelse af effektivitet og besparelser

Beskrivelse

Det offentlige udsteder en lang række forskellige beviser til borgerne. Uden nogen krav på fuldstændighed kan nævnes:

- kørekort
- jagttegn
- fiskekort (girokvittering)
- sygesikringsbevis

- medicintilskudskort til pensionister
- lånerkort til biblioteker
- skattekort.

Sådanne personlige beviser kan opbevares i et borger ic-kort. Eksistensen af beviset og evt. indhold heraf kan aflæses på terminaler - der også kan være håndbårne. Ved at benytte den kortindehaver-identifikation, der findes på kortet, kan der gennemføres en meget sikker dokumentation af, at den, der har beviset, er dets retmæssige indehaver.

Der udnyttes to funktioner i kortet dels som databærer med oplysninger om beviset og dets nærmere indhold og dels kortindehaver-identifikationen til verifikations-proceduren.

Vurdering

Der er en udvikling i gang, hvor forskellige beviser gøres elektronisk læsbare, f.eks. sygesikringsbeviset og lånerkort. Denne overgang til elektronisk læsbare beviser sker ikke ud fra en standard eller samlet plan. Borgerne får derfor en række beviser, i stedet for et/få med en standardiseret brugergrænseflade.

Ved at anvende et borger ic-kort vil man sikre en meget stærk verifikation af om den, der ønsker at benytte det pågældende bevis er dets indehaver. Men man må for det enkelte bevis spørge, om der egentlig behøves en så sikker kortindehaver-identifikation?

Hvis det personlige bevis indlægges på et borger ic-kort vil det sandsynligvis være et problem, at det næppe kan gøres visuelt, at kortet indeholder pågældende bevis. Man vil derfor samtidig være nødt til at udstede et papirbevis.

En række beviser, f.eks. pas og kørekort, vil man som følge af international anvendelse og internationale aftaler ikke kunne lade afløse af en elektronisk version på borger ic-kortet.

En anden udviklingsmulighed er, at man i forhold til elektronisk behandling af personlige beviser ikke behøver at opbevare dem på kortet. I stedet benytter man borger ic-kortets funktion som brugeridentifikation til at slå op i et edb-register og her konstatere om personen er i besiddelse af det personlige bevis og det nærmere indhold heraf. Der ligger ikke heri, at der opbygges ét centralt personregister med alle oplysninger, men en fortsættelse af den nuværende udvikling, med edb-registre hos den enkelte myndighed. Disse registre vil naturligvis i øvrigt blive anvendt til den administration der er knyttet til myndighedens arbejde. På denne måde kunne man bevare forskellige beviser, der anvendes manuelt og til den utvivlsomt øgede elektroniske kommunikation anvende en generel fremgangsmåde, som er til stede i borger ic-kortet.

Det må således sammenfattende vurderes, at det ikke er hensigtsmæssigt at indlægge personlige beviser på et borger ic-kort.

c) Generel helbredsjournal

I dette anvendelses-eksempel opbevares en journal med helbredsoplysninger på kortet.

Mål

* Umiddelbar adgang til en række helbredsoplysninger
* Adgang til helbredsoplysninger i situationer, hvor der ikke er adgang til datanet. Kan behandles i stand-alone systemer.
* Borgeren/patienten har en egen kontrol med og overblik over sin journal

Beskrivelse

I en interim rapport fra den europæiske standardiseringsorganisations arbejdsgruppe om sundhedskort (CEN TC251/WG7) gøres en foreløbig status på, hvilke kliniske data, som kan opbevares på et sundhedskort. Der peges med en række brede termer bl.a. på følgende data:

Symptoms
Signs
Examination findings
Investigations
History details (present history, social history)
Operations
Procedures

Diagnostic information
Laboratory data
Allergies/sensitivities
Dietary details
Emergency Health record data.

Personen vil på denne måde have en ret omfattende journal med helbredsoplysninger og data fra kontakter med sundhedsvæsnet.

Vurdering

Man kan tænke sig, at en sådan helbredsjournal skal afløse journaler hos læger, hospitaler osv. En sådan situation rejser en række problemer i forhold til anvendelsen af journalen, når patienten ikke er til stede, og ved anden anvendelse af journaler f.eks. til ressourcestyring og kvalitetssikring. Desuden er der problemer med at sikre, at dataene ikke går tabt.

En anden mulighed er, at journalen er personens private kopi eller databank med helbredsoplysninger. Derved er der ikke problemer for sundhedsvæsnet i forhold til manglende journaler. Et centralt problem her vil være opdatering og sletning af uaktuelle og forældede data. Omvendt kan man opbevare data på kortet, som af register-hensyn slettes hos sundheds-institutionerne.

I CapSesa rapporten til EF's AIM-projekt vurderes det, at der ikke foreløbig vil kunne skabes accept af generelle kort (dvs. de næste 10-20 år).

Det kan ikke entydigt vurderes om det vil være hensigtsmæssigt at opbevare en generel helbredsjournal på et borger ic-kort.

d) Specialiseret helbredsjournal

I dette anvendelses-eksempel opbevares en journal over en særlig og helbredsmæssig vigtig sygdom hos personen.

Mål

* Bedre og hurtigere diagnose for patienten
* Bedre og mere sikker nødbehandling gennem adgang til en medicinsk journal
* Adgang til journal uden adgang til datanet, f.eks. i udlandet
* Personen/ patienten har en egen kontrol med og adgang til sin journal

Beskrivelse

På kortet opbevares en specialiseret journal over en sygdom. Det kan f.eks. være: diabetes, cancer, bløder, astma, hjertesygdomme. Journalen opdateres ved behandling og kontrol hos den primære behandlings-institution. Journalen er tilgængelig ved alle henvendelser i sundhedssektoren og kan benyttes til vurdering af, om der skal tages særlige hensyn. I et EF-perspektiv vil det også betyde, at journalen er tilgængelig ved rejser rundt i EF-landene. Endvidere vil journalen være tilgængelig f.eks. i en ambulance i forbindelse med en nødsituation.

Vurdering

Da der for den enkelte sygdom er tale om et begrænset datasæt er det mere realistisk, at der skabes den fornødne standardisering mv., som er en forudsætning for at journalen kan etableres.

Den specialiserede journal må ses som et supplement til hospitalets journal, idet den er personens private journal. Der er tale om en afgrænset persongruppe, som har en stærk egeninteresse i at oplysningerne er tilgængelige og korrekte. Man kan forestille sig, at den enkelte selv skal anmode om/tillade, at journalen indlægges på beviset, og at adgangen til journalen forudsætter, at personen giver adgang via sin adgangskode. Der bør endvidere findes en særlig autorisation af det personale, som skal benytte terminalen, hvor dataene skal læses.

I CapSesa rapportens konklusioner peger man på, at der bør satses på at udvikle specielle medicinske records til kroniske sygdomme på ic-kort. I EF har man gennemført et projekt, DIABCARD, om opbevaring af helbredsoplysninger om sygdommen diabetes, og der er andre tilsvarende projekter i gang bl.a. om cancer.

Det må sammenfattende vurderes, at en specialiseret helbredsjounal kan etableres på et borger ic-kort.

e) Vandrejournal i sundhedssektoren

I dette anvendelses-eksempel opbevares en vandrejournal som anvendes af læger og sundhedsinstitutioner mv.

Mål

* Elektronisk overførsel og opdatering af vandrejournal
* Sikre personen en egen kontrol med sin journal
* Mulighed for at journalen læses uden for sundhedsnettet

Beskrivelse

I en række forløb oprettes en journal som bæres rundt til forskellige instanser. Som eksempler kan nævnes en barsel og en arbejdsskade.

Ideen er den oplagte, at journalen kan indlæses elektronisk og opdateres ved kontakt med forskellige sundhedsinstitutioner. Hos læge, hospital osv. kan opdatering af evt. egen journal og vandrejournalen ske i én arbejdsgang.

Vurdering

Efterhånden som anvendelsen af edb bliver almindelig i alle instanser vil det være hensigtsmæssigt, at sådanne journaler også kan læses og opdateres elektronisk. Det kan selvfølgelig ske ved anvendelse af et sundhedsnet og datatransmission, men det vil betyde at pågældende person så at sige bliver koblet fra. Ved at åbne mulighed for at indlægge journalen på personens kort bliver vedkommende inddraget i denne kommunikation og bevarer en kontrol over sin journal.

Det er i personens egen interesse, at journalen er tilgængelig og korrekt, hvorfor betingelserne for høj datakvalitet er til stede.

Sammenfattende kan det vurderes, at en vandrejournal kan etableres på et borger ic-kort.

f) Recepter/medicinforbrug

I dette anvendelses-eksempel opbevares recepter til apoteket og en record med medicinforbrug.

Mål

* Valgfrihed ved brug af apotek (i.f.t. elektronisk overførsel af recept)
* Opbevaring af recepter, der kan benyttes flere gange
* Give grundlag for interaktions-kontrol
* Kontrol af gentagelses receptudstedelse

Beskrivelse

På kortet findes mulighed for at opbevare en recept, der f.eks. udstedes af en praktiserende læge. Ved henvendelsen til apoteket kan recepten indlæses elektronisk i dets edb-system. Opbevaring af recepter på kort kan ses som et supplement til anden overførsel af recepter fra lægen til apoteket. Det giver personen en valgfrihed. Endvidere kan man opbevare recepter, der giver adgang til flere udleveringer på kortet.

I fortsættelse af denne anvendelse vil det være oplagt at kunne opbevare data om medicinforbrug (tidligere udleveret medicin - recept eller håndkøb - og medicin der benyttes for tiden). Disse data vil kunne give mulighed for at foretage en såkaldt interaktions-kontrol hos lægen og på apoteket. Lægemiddelinteraktion betyder at forskellige lægemidler på en eller anden måde har en uheldig/uønsket effekt over for hinanden.

Adgang til dataene kan kun ske efter personen har givet tilladelse med sin adgangskode.

Endelig kunne man i bestemte situationer over for misbrugsgrupper kræve, at udleverede medikamenter blev registreret på kortet, og at lægen/apoteket fik adgang hertil, før der skete fornyet udlevering.

Vurdering

Der er fra forskellig side peget på muligheder for at benytte ic-kort til sådanne anvendelser. Der er tale om begrænsede datamængder og dataene vil kunne opbevares på borger ic-kortet.

Undersøgelser har vist at der faktisk udleveres medicin som har interaktionsproblemer og at en del (ca. 10%) hospitalsindlæggelser kan henføres til det, der kaldes lægemiddelrelaterede indlæggelser. Endvidere ønsker man generelt at gøre overførsel af recepter elektronisk med henblik på betydelige besparelser.

Ved opbevaring af recepter og medicinforbrug er der tale om et frivilligt tilbud, og data indlægges kun med personens accept. Problemer med datakvalitet og backup må derfor forventes at kunne håndteres.

Anvendelsen til kontrol med udlevering af medikamenter rejser spørgsmål i forhold til anvendelse af borger ic-kortet til kontrolformål og hvorvidt det skal være muligt at kræve data på kortet udleveret.

g) Nød-/advarselsoplysninger

I dette anvendelses-eksempel opbevares en række afgrænsede helbredsoplysninger, som kan have betydning i en nødsituation.

Mål

* Hurtig adgang til centrale helbredsoplysninger

* Adgang til oplysningerne i præ-hospital behandling, specielt ambulancer.

Beskrivelse

På borger ic-kortet opbevares en række helbredsoplysninger, som kan være af betydning i en nødsituation eller være vigtige at advare om i en behandlingssituation. Da der er tale om begrænsede oplysninger, der sandsynligvis kan findes som koder, vil de kunne opbevares på borger ic-kortet. Det første oplagte anvendelsessted er i ambulancen i forbindelse med ulykker og akut indlæggelse. Men også i anden præ-hospital behandling af vagtlæger, hjemmeplejer og praktiserende læger kan oplysningerne være anvendelige.

I en række situationer bør der i sagens natur være adgang til disse data, uden at personen giver tilladelse hertil med sin kode. Det bør i systemopbygningen sikres, at dataene kun kan læses af personer der er autoriseret hertil.

Vurdering

Ønsket om at opbevare nød/advarselsoplysninger blev omtalt i bemærkningerne i forslaget til en sundhedslov, som blev fremsat i 1992, men ikke vedtaget. Det hedder: "Sundhedskortet kan tillige åbne mulighed for med de berettigedes samtykke at registrere vigtige helbredsoplysninger om f.eks. kroniske sygdomme, allergier, blodtype, vaccinationer, samt eventuelle organdonortilsagn til brug under akutte omstændigheder." For oplysninger om kroniske sygdomme o.lign. kan der være tale om en henvisning til en specialiseret journal.

Muligheden for at opbevare sådanne helbredsoplysninger på sit kort kan man betragte som et tilbud til borgerne, der dog må antages at have en stærk egeninteresse i at få oplysningerne lagt ind på kortet.

h) Arbejdsløses sagsjournal

I dette anvendelses-eksempel opbevares en sagsjournal med oplysninger, der indgår i den lediges sag i forhold til AF, myndigheder, A-kasse o.l.

Mål

* Sagsoplysninger skal være til stede, når de er relevante for en instans som har en rolle i forhold til rådgivning af den ledige.

* Den ledige skal have en aktiv rolle i forhold til sine oplysninger og kunne styre hvilke data der frigives til sekundære vejlednings-centre.

Beskrivelse

I sagsjournalen opsamles data fra den lediges kontakt med AF, A-kasse, kommune m.fl. Der opbevares de data, der idag registreres i AF-Match og i A-kasserne (bortset fra data vedr. dagpengeudbetaling). Disse data vil derfor ikke længere skulle registreres i deres egne registre.

Dataene på borger ic-kortet befinder sig hos borgeren og kan anvendes i sammenhænge, hvor hun henvender sig og ønsker assistance fra "instanserne". Den ledige kommer i kontakt med mange forskellige organisationer ved et længere ledighedsforløb. Kun mellem AF og A-kasse er etableret en elektronisk dataudveksling, der dog ikke omfatter alle data. Antallet af instanser kan forudses at stige, og samtidig er det ikke hensigtsmæssigt at etablere dataudveksling mellem alle instanser.

Ved møder på AF, A-kasse og andre vejlednings-centre kan kortet anbringes i en kortlæser og (relevant) indhold kan læses på en terminal. Der kan herefter ske en opdatering af indholdet.

Sagsjournalen fungerer som den lediges dokumentation for indhold og resultater af kontakten med AF og A-kasse. Den enkelte vil hjemme kunne se på "sagen". Der kan være mulighed for at personen tilføjer oplysninger, der mangler eller hvor der er sket ændringer, og hun kan slette oplysninger, der er uaktuelle.

Sagsjournalen vil endvidere kunne anvendes ved kontakt med andre vejledningscentre, f.eks. uddannelsesinstitutioner og kommunen (bistandskontoret, beskæftigelsessekretariatet).

Vurdering

En sagsjournal vil for så vidt kunne opfylde de to skitserede mål.

Det var dog opfattelsen såvel i AF-regionen som i SiD/A-kassen, at de oplysninger der i dag findes i registrene ikke kan undværes eller flyttes over på et kort hos den ledige. Oplysningerne bliver anvendt på forskellig vis i sagsbehandlingen, også når den ledige ikke er til stede.

AF understregede, at disse oplysninger er ryggraden i AF's opgaver. Oplysningerne er simpelt hen grundlag for formidlingen af ledige. Og dernæst er oplysningerne grundlag for den overvågning af arbejdsmarkedet og de analyseaktiviteter, AF gennemfører med henblik på tilrettelæggelse af uddannelse osv.

SiD-Roskilde fremhævede, at man faktisk havde som målsætning at minimere den tid medlemmet måtte være til stede, for at man kunne sagsbehandle hans sag. Derfor søger man at afklare sagen mens medlemmet er til stede, for efterfølgende at færdigbehandle den. Endvidere anvender arbejdsløshedskassen f.eks. oplysningerne i edb-registeret til med kort varsel at finde personer til et kursus, hvor der blevet nogle pladser ledige.

Det må derfor vurderes, at der ikke inden for det nuværende system vil være mulighed for at indføre en sagsjournal i det her overvejede omfang.

i) Arbejdsløses vandrejournal

I dette anvendelses-eksempel anvendes borger ic-kortet til opbevaring af visse data i forbindelse med et ledighedsforløb. Dataene er en kopi af data, der er registreret i A-kassen og i AF. Vandrejournalen fungerer som den lediges kopi/dokumentation og kan bruges af alle relevante vejlednings-centre.

Mål

* Sagsoplysninger skal være til stede når de er relevante for en instans, som har en rolle i forhold til rådgivning af den ledige.

* Den ledige skal have en aktiv rolle i forhold til sine oplysninger og kunne styre hvilke data der frigives til sekundære

vejlednings-centre.

Beskrivelse

I vandrejournalen opsamles data fra sagsbehandlingen af den ledige. Med den nuværende ledighed (1. kvt. 1993) er ca. 800.000 ledige i en vis periode. Omkring 100.000 er ledige i mere end 3 måneder og ca. 20.000 ledige i mere end 18 måneder. Man kunne forestille sig, at vandrejournalen blev oprettet ved den første større kontakt med AF, f.eks. ved 3 månederssamtalen.

Vandrejournalen kan indeholde data som angivet i skemaet.

Ved møder på AF, A-kasse og andre vejlednings-centre kan kortet anbringes i en kortlæser og (relevant) indhold kan læses på en terminal. Der kan herefter ske en opdatering af indholdet. På AF/A-kasse vil denne opdatering kunne ske automatisk i forbindelse med indrapportering til eget system.

Vandrejournalen fungerer, som den lediges dokumentation for indhold og resultater af kontakten med AF og A-kasse. Den enkelte vil hjemme kunne se på "sagen". Der kan være mulighed for at personen tilføjer oplysninger, der mangler eller hvor der er sket ændringer, og hun kan slette oplysninger der er uaktuelle. Disse oplysninger kan herefter opdateres ved næste kontakt med AF/A-kasse.

Vandrejournalen fungerer som bidrag til udveksling af korrekte data mellem AF og A-kassen, idet indholdet kan benyttes til opdatering.

Vandrejournalen fungerer som muligt grundlag i den lediges kontakt med andre "instanser": f.eks. kommunen, AMU, uddannelsessteder. Det forudsættes, at der ved personbeviset er etableret en adgangskontrol, således at kort-indehaveren styrer, hvilke data der frigives, og en

Vandrejournal		
gruppe	beskrivelse	fra
Stamoplysninger	AF-kontor/A-kasse Forsikringskategori	
Kommune	Henvisning fra kommune Kontrolkort	
Sagsoplysninger	Tilmelding(er) AF: dato Ledighed, timer Seneste beregnede falddato Kontakt med AF/A-kasse Oplysninger vedr. arbejdstilbud	
Vejlednings-oplysninger	Tidligere beskæftigelse Uddannelse Fagønsker Uddannelse/kursusønsker Uddannelsesplaner og -aktivitet	
Særlige oplysninger	Evt. fritekster fra AF/A-kasse Særlige forhold (ex. helbredsoplysninger)	
Bemærkninger:		

adgangskontrol, således at kun autoriserede personer kan få adgang til bestemte relevante data.

Vurdering

Vandrejournalen vil kunne opfylde de angivne mål. Den er - i modsætning til h) sagsjournalen - ikke i strid med hensyn hos AF og A-kasser om at have dataene til rådighed. Andre instanser har ikke opbygget registre med disse data og etableret dataudveksling, og de vil opleve en forbedring af deres adgang til relevante data.

Det kan vurderes, at der er mulighed for denne anvendelse på et borger ic-kort.

Supplerende kan det tilføjes, at et centralt punkt i de ændringer, som trådte i kraft 1. januar 1994, er oprettelse af en individuel, konkret handlingsplan, som den ledige har ret til. Handlingsplanen skal aftales med AF, men skal udarbejdes i samarbejde med andre instanser: A-kasse, kommune, uddannelsessteder og vil blive et omdrejningspunkt i vejlednings-indsatsen over for de ledige. En sagsjournal ville oplagt kunne indeholde denne handlingsplan, og dermed gøre den tilgængelig hos forskellige instanser, uden at der dermed skal opbygges datatransmission mellem dem.

j) Uddannelsesdata

I dette anvendelses-eksempel opbevares uddannelses-data på borger ic-kortet, der fungerer som en privat databank med oplysninger man ellers skal gemme og medbringe i forskellige sammenhænge.

Mål

* Uddannelsesdata opbevares på en enkel måde og kan gøres tilgængelig når der er behov.

Beskrivelse

Dokumentation for bestået uddannelse, gennemførte kurser og erhvervede certifikater spiller en stigende rolle på arbejdsmarkedet. For stadig flere funktioner på såvel specialarbejderområdet som på faglærte arbejdsområder kræves certifikater for bestemte færdigheder.

Med den stadig stigende betydning af uddannelse - og fortsat efter- og videreuddannelse - vil stadig flere borgere opsamle en række uddannelser af forskellig art, som der kan være behov for at kunne dokumentere ved forskellige lejligheder.

På borger ic-kortet kan opbevares data om gennemført uddannelse af enhver art. Data på kortet kan opdateres af uddannelsesinstitutioner og af borgeren selv. For uddannelser, der afsluttes med udstedelse af eksamensbevis, certifikat eller lignende, kan beviset signeres med en elektronisk-signatur. Uddannelse, kurser m.v. som ikke er kompetencegivende, kan borgeren selv indrapportere.

Uddannelses-data fungerer som en privat databank (eller arkiv) over de uddannelser den enkelte har gennemført. I lighed med ens private arkiv hjemme må det være frit for den enkelte at slette bestemte uddannelsesdata og kunne styre hvilke uddannelses-data, der kan læses i en konkret sammenhæng.

Uddannelses-data kan fungere som dokumentation over for

- AF og A-kasse i vejledning af ledige
- andre vejlednings-centre for ledige
- arbejdsgivere ved ansættelse og udførelse af arbejdsfunktioner der f.eks. kræver certifikater
- uddannelsesteder, hvor der er bestemte adgangsbetingelser
- tillidsrepræsentanter, der på fagforeningens vegne fører opsyn med de faglige kvalifikationer.

Ved kontakt med uddannelsessteder kan kortet anbringes i en kortlæser, og (relevant) indhold kan læses på en terminal. Der kan ske en opdatering af indholdet, og signatur kan indlægges.

Vurdering

En opbevaring af uddannelses-data på et borger ic-kort vil opfylde det opstillede mål.

Det skal bemærkes, at målet er bredere end løsning af problemer for den ledige i forbindelse med vejledning. Dette snævrere mål vil også blive opfyldt, og man vil endog kunne bygge på, at disse data allerede er til stede.

Det kan vurderes, at der er mulighed for denne kort-funktion for et borger ic-kort.

4.G Brugerbetaling

En brugerbetaling for en offentlig service kan opbygges efter forskellige principper:

- kontant betaling sammen med ydelsen, som kan ske med almindelige penge, en check eller elektronisk. Borger ic-kortet kan anvendes til at opbevare elektroniske penge, identifikation til bankkonto og til administration af særlige beregningsregler for det opkrævede beløb,

- forudbetalt i form af et gebyr, klippekort eller et periodekort. Borger ic-kortet kan anvendes til at opbevare dokumentation for forudbetalingen og fungere som klippekort,

- konto- eller kreditordning med periodevis kontoopgørelse og opkrævning af betaling. Borger ic-kortet kan her anvendes til brugeridentifikation og til administration af særlige betalings-regler.

I dette afsnit behandles tre anvendelses-eksempler

a) Penge
b) Admininistrationsregler
c) Vejafgifter

a) Penge

I denne anvendelse opbevares elektroniske penge på kortet til betaling af offentlige ydelser/service.

Mål

* Lette betaling for offentlige ydelser

Beskrivelse

På kortet indlægges et beløb, som efterhånden som det anvendes til betalinger tælles ned. Ved de enkelte anvendelser foretages ikke en kortindehaver-identifikation, dvs. kortets beløb kan benyttes af den som har kortet i hånden. Beløb på kortet kan tænkes indlagt i automater, der opstillet i pengeinstitutterne og andre steder. Denne betalingsmåde kan tænkes anvendt på områder, hvor der i dag sker en betaling - f.eks. entré til museer og svømmehal - eller overvejes på nye områder.

Vurdering

Etablering af en sådan betaling af mindre beløb vil utvivlsomt være en rationalisering for administrationen, og det kan også betragtes som en forenkling for borgeren.

Det er i dag ikke nødvendigt at udnytte et offentligt borger ic-kort for at skabe et sådant forudbetalt betalingskort. DANMØNT, som PBS og KTAS står bag, er i fuld gang med at opbygge et åbent system med forudbetalt pengekort. Kortet er tænkt som et småpengekort og udstedes med beløb op til 300 kr. De nuværende DANMØNT kort ikke genopladelige, dvs. de kasseres når pengene er brugt. Men man planlægger at kunne tilbyde kort der kan genoplades, i 1994/95 [45].

Det må derfor anses for helt udelukket, at man etablerer et særligt (lukket) penge-system i den offentlige sektor.

Men spørgsmålet er mere generelt, om det overhovedet ville være en god ide, at opbevare penge i en eller anden form på et borger ic-kort. På den ene side vil man på borger ic-kortet opbevare noget der - uanset om der er tale om mindre beløb - er værd at stjæle, da kortet umiddelbart kan bruges, fordi der ikke kræves kortindehaver-identifikation når pengene bruges. På den anden side har vi et borger ic-kort, som bestemt ikke bør mistes ved tyveri, og hvor man ved en effektiv kortindehaver-identifikation forsøger at gøre det uinteressant at stjæle kortet, fordi det ikke kan bruges. Denne kombination af anvendelser må helt afvises. Det må generelt vurderes, at borger ic-kortet ikke bør have kort-funktioner til anvendelser, hvor der er tale om ihændehaverkort,

dvs. der ikke er anden kortindehaver-identifikation, end at man har kortet i hånden. Det bør tilføjes, at man ikke bør flytte sikkerhedsniveauet fra ihændehaverkort til krav om kortindehaver identifikation alene for at kunne bruge et borger ic-kort.

b) Administrations-regler

I denne anvendelse benyttes kortet til at gennemføre en eller anden form for administration af en brugerbetaling [46].

Mål

* Gennemføre en brugerbetaling som forudsætter en administration og beregning.

Beskrivelse

Hvis man vil indføre en brugerbetaling, som forudsætter en beregning og/eller opbevaring af oplysninger som grundlag for, hvad der skal betales, kan borger ic-kortet anvendes. Når borgeren modtager den ydelse, der skal betales for, afgiver service-udbyderen oplysninger til kortet, som foretager en beregning af, hvad der skal betales og lagrer evt. oplysninger, som skal benyttes igen næste gang. Som første led skal der ske en kort-indehaver identifikation.

Som eksempel kan nævnes den egenbetalingsgrænse på 800 kr. ved medicinindkøb som indførtes i 1988 - og senere blev ophævet bl.a. pga. de store vanskeligheder ved at administrere den. En sådan regel ville meget enkelt kunne administreres ved anvendelse af borger ic-kortet. Her kunne løbende indlægges beløb for indkøbt medicin, og apoteket kunne få svar på, om der kunne ydes tilskud eller ej.

Når der skal ske en beregning ved administrationen af kortet, er der mulighed for at indlægge kriterier af forskellig art for denne beregning. Der kan f.eks. være tale om kvantitetskriterier (efter en vis mængde forbrug skal der ske betaling; eller en mængde rabat), eller sociale kriterier således at betalingen er differentieret på baggrund af indkomst og anden social situation. I eksemplet med egenbetalingsgrænsen ville det være muligt at indlægge en individuel egenbetalingsgrænse på 0 kr. eller 400 kr.

Vurdering

Et borger ic-kort giver mulighed for at indføre forskelligartede administrationsordninger af en brugerbetaling.

Anvendelse af et borger ic-kort giver nogle særlige muligheder for tilrettelæggelse af ordningen. I og med beregning og opbevaring af oplysninger kan ske i kortet kan man undgå central registrering af borgernes forbrug. Hvis der indlægges sociale kriterier i beregningen, kan anvendelsen tilrettelægges, så det ikke er synligt for andre, at der findes sådanne kriterier i beregningen.

Anvendelsen af en administrations-ordning kan også kombineres med en konto-ordning, hvor man kan forestille sig, at der på baggrund af oplysninger i kortet foretages en beregning af hvad der skal betales, og først derefter sendes oplysninger til edb-systemet.

Hvis der som led i en administration løbende opdateres data i kortet, som har betydning fremover, opstår der et back-up krav. Består administrationen alene i en beregning - evt. med særlige kriterier - giver det ikke særlige backup problemer idet disse data vil kunne genindlægges af myndigheden på et nyt kort.

c) Vejafgifter

I denne anvendelse benyttes borger ic-kortet til betaling af bilkørsel på bestemte veje.

Mål

* At gennemføre en vejafgift (bompenge) på en enkel måde

Beskrivelse

Betaling for kørsel på bestemte veje ("bompenge"), f.eks. betaling for kørsel på motorveje eller betaling ved indfaldsveje til byområder diskuteres med mellemrum. I de store broprojekter på Storebælt og Øresund er betaling for kørsel over broen en forudsætning for finansieringen.

Et automatisk betalingssystem kan med anvendelse af et ic-kort etableres på følgende måde:

Det er muligt at gennemføre betalingen medens bilen passerer i almindelig fart. I bilens forrude findes en terminal, hvor borger ic-kortet kan anbringes og kortindehaver-identifikation foretages. Terminalen kan ved hjælp af infrarøde stråler eller radiobølger etablere en datakommunikation mellem bilen og antenner i luften eller ved siden af vejen, som udgør betalings-stedet. Betalings-stedet består af to aflæsere og et edb-system. Når bilen passerer den første aflæser registreres bilisten med oplysninger fra borger ic-kortet (f.eks cpr-nummer), og der sendes besked til terminalen om betaling. Herefter tæller terminalen klippekortet ned eller kontrollerer, at der er betalt for pågældende dag (periodekort). Ved næste aflæser meddeler terminalen i bilen, at betalingen er OK og vejafgift-systemet sletter sin registrering af bilisten. Modtages der ikke besked om betaling bevares registreringen - evt. foretages en fotografering - med henblik på regning og gebyr/bøde. Hvis klippekortet nærmer sig nul, giver terminalen besked til bilisten. For at sikre at uvedkommende ikke kan tappe, hvem der passerer betalingstedet, kan kommunikationen mellem bilen og aflæsestederne ske krypteret.

Et sådan automatisk betalingssystem vil have mange fordele (mindre pladskrav, ingen mandskab, ingen forsinkelser i trafikken) i forhold til klassiske vejafgift-systemer. Endvidere vil systemet kunne gennemføre en differentieret opkrævning. F.eks. kan kørsel ind til en storby i myldretiden koste flere klip end kørsel på andre tidspunkter.

Vurdering

Et borger ic-kort kan have en kort-funktion til denne type brugerbetaling.

Da anvendelsen, som den er beskrevet her, forudsætter kortindehaver-identifikation vil der ikke indføres en tyvetækkelig situation, jf. vurderingen i afsnit a ovenfor.

Der er mulighed for at indføre forskellige typer kriterier (alder, pensionist, indkomst) for betalingen af vejafgiften i kortet uden det i forbrugssituationen er synligt. Kriterierne kan evt. indlægges som en beregning, der skal foretages, når det forudbetalte beløb opdateres.

Det må vurderes, at der ikke er et back-up problem ved denne anvendelse. Hvis kortet mistes må ubrugte bompenge anses for tabt.

[23] Göran Gohlkuhl/Annie Röstlinger: Förändringsanalys. Arbetsmetodik och förhålningssätt för goda förändringsbeslut (1988).

[24] I en dom afsagt af Retten i Roskilde den 15. oktober 1987 blev udsagn fra PBS' sikkerhedschef om systemets sikkerhed lagt til grund for en afgørelse, om at et antal træk med Dankortet var foretaget. Trykt i Mads Bryde Andersen: EDB-Ret, Lovgivning, Retsafgørelse, Kontrakter (1991) s. 128.

[25] AKF-nyt: Selvbetjening af service - nu eller aldrig? nr. 1 1991 s. 23-28.
Danske Kommuner: Velkommen til selvbetjeningssamfundet. nr. 9-1993 s. 5-9.
Halldór Færch og Ivan Norling: Egenservice. Kommunedata 1991
LO: Kommunal service - på nye måder. I: Med Teknologien på vej (1992) s. 27-37.

[26] Denne funktion er en del at en svensk sikkerhedsløsning for pc'er.
Funktionsspecifikation: Allterminalen: En säkerhetslösning för persondatorer. 1993-09-24.
Introduceret i Claus Engelund og Steffen Stripp: Pc-sikkerhed hinsidan. PROSA-bladet nr. 2-1994.

[27] Datapost400: Hvad er X.400. TeleCOM

[28] Mogens Kühn Pedersen: EDI i Virksomheden (1990).

[29] Peter Landrock: Elektroniske dokumenter. Ugeskrift for Retsvæsen B 1992 s. 176-180.

Charles F. Pleeger: Security in Computing (1989).

[30] Telestyrelsen: Hovedrapport vedrørende et eventuelt myndighedsinitiativ på krypteringsområdet (1993).

[31] PBS: Digital Signature, TeleSec - a total solution to secure EDI transactions. (Upubl. 1992)

[32] Commission of The European Communities, DGXIII: Collaboration in the field of Electronic Signature. INFOSEC Workplan '94

[33] Bent Okholm: Elektronisk Signatur og kryptografering. (Upubl 1990). Beskrivelse af et produkt.

[34] X.509: The Directory - Part 8: Authentication framework.

[35] Chryptomathic: TEDIS II, B7, Security 2: Security in Open Environments s. 3

[36] Dansk Standard Inf. 43: Kryptografi & Datasikkerhed (1988).
Charles F. Pleeger: Security in Computing (1989).

[37] Primært udarbejdet på baggrund af drøftelser med socialrådgiver Anne-Lise Mathiasen, Græsted-Gilleje Kommune

[38] Kommunernes Landsforening: Fuldført sagsbehandling med små edb-ressourcer. I Når edb gi'r gevinster (1990).

[39] Kommunernes Landsforening: Kvik, kvikkere, kvikskranke. (1991).

[40] Peter Blume: Personregistrering (1992).
Steffen Stripp: Registerlovene (1992).

[41] TeknologiNævnets registergruppe: Hvem ved hvad - og bør de det? (1993).

[42] Halldór Færch og Ivan Norling: Egenservice. Kommunedata (1991) s. 47.

[43] Bekendtgørelse om ledige arbejdsløshedskassemedlemmers kontakt med arbejdsformidlingen af 30. nov. 1990. Cirkulære om ledige arbejdsløshedskassemedlemmers kontakt med arbejdsformidlingen af 10. dec. 1990.
Bekendtgørelsen om en arbejdsløshedskasses vejledningspligt overfor dens medlemmer af 18. maj 1989
Oversigt over de informationer der udveksles mellem arbejdsløshedskasserne og Arbejdsformidlingen til brug for vejledningen af ledige arbejdsløshedskassemedlemmer (bilag 1 til rådighedsbekendtgørelsen nr. 673 af 9. okt. 1991)
Brev fra AMS til regionerne af 14. jan. 1992: Vedrørende edb-mæssig udveksling af informationer mellem A- kasserne og AF.
Registerforskrift for AF-MATCH.
Det skal bemærkes at undersøgelsen bygger på lovgivningen før ændringerne, der trådte i kraft 1. januar 1994.

[44] Lars Toft(red): Videreudvikling af sygesikringsbeviset. Rapport Amtsrådsforeningen i Danmark. (1990)
CapSesa: Preparation of a European Strategic Action for the use of "Data Cards" in the health care domain. AIM DG XIII (1993).
Den elektroniske patientjournal m.m. i Danmarks Amtsråd nr. 11 29. juni 1993
Knut Bernstein, Helga Sigmund: Elektronisk Datakommunikation i sundhedssektoren. DSI-rapport 92.04 (1992).
Mette Bjørn m.fl.: Edb-recepter - Amagerforsøget. Farmaceuten 4/1991
Michael Voel Jensen: Edb på mange fronter. Farmacia 92 s. 202-204
Henrik Bjerregaard Jensen: Elektronisk datakommunikation i den fynske sundhedssektor. Overheads fra seminar 5. marts 1992.
Forslag til lov om det offentlige sundhedsvæsen. L74 af 30. oktober 1991
Shahid Baig: Patient Data Cards. XIII Magazine 1992
Teknologi skal gøre den gode terapi bedre. Apotekerforeningens blad.

[45] Upubliceret materiale fra DANMØNT A/S

[46] Rapport fra Amtsrådsforeningen: Videreudvikling af sygesikringsbeviset (1990)
Uffe Paludan og Christian Lotz: Brugerbetaling i et pengeløst samfund i Berlingske Tidende 29/6-89.

[47] M. Devargas: Smart Cards and Memory Cards. NCC (1992) afsnit 5.5: Road-toll debit Card s. 49-52
Steen Lauridsen: Brugerbetaling på vejene. vdl-nyt nr 3 1991 s. 22-23.

5. Sikkerhed

I dette afsnit behandles en række forhold om sikkerhed ved et borger ic-kort system. I forhold til spørgsmålet om vi danskere skal have et borger ic-kort er edb-sikkerhed en nødvendig, men ikke tilstrækkelig betingelse. Kun hvis der kan opnås en tilstrækkelig høj sikkerhed for kortet, en anvendelse eller kortsystemet som helhed, kan borger ic-kortet eller anvendelsen accepteres.

Edb-sikkerhed etablerer sikkerhedsforanstaltninger, som skal sikre:

integritet:	at kortet, anvendelser og systemer fungerer uden fejl og at alle data er korrekte,
tilgængelighed:	at man til stadighed kan benytte kortet, anvendelser og systemer og få adgang til data,
fortrolighed:	at adgangen til data på kortet og i edb-systemer kan kontrolleres så uvedkommende ikke får mulighed for at se eller ændre dataindholdet.

I de følgende afsnit diskuteres først generelt krav til sikkerheden. Dernæst behandles en række hændelser som rejser sikkerhedsproblemer. Og endelig behandles sikkerhed ved kortet, kortindehaver-identifikation, kortlæser og kommunikation.

Selv om det alene er kort-systemet, som behandles her, skal det understreges, at det samlede systems sikkerhed ikke er bedre end det svageste led. Derfor skal edb-systemer hos offentlige myndigheder og private virksomheder, som kortindehaveren kommunikerer med, også opfylde de krav til sikkerheden, som behandles i afsnit a) nedenfor. Det vil ikke blive nærmere behandlet, hvordan denne sikkerhed kan opnås.

Endvidere skal det bemærkes, at sikkerhed er et fælles ansvar, som omfatter alle aktører: leverandører af produkter og programmer, kortsystem operatøren, edb-system ansvarlige, brugere og kort-indehavere.

a) Kvalitetskrav

Med kvalitet menes her kort-systemets "egenskaber og karakteristiske træk - set som helhed - som har noget at gøre med dets evne til at opfylde specificerede eller underforståede behov" (DS/ISO 8402: Kvalitet - ordliste). Ved edb-systemer (software) forsøges kvaliteten specificeret med en række egenskaber. ISO-standarden, "Information technology - software product evaluation" definerer en række "software quality characteristics" (kvalitetsegenskaber) og i et bilag forslag til uddybende "sub-characteristics" (IS9126). Flere egenskaber har direkte betydning for sikkerheden:

- hemmeligholdelse af programmer og data (security)
- pålidelighed, virker det hver gang? (reliability)
- reetablering, muligheder for at genstarte efter fejl (recoverability).

Umiddelbart kunne man stille kravet 100% sikkerhed, men af en række grunde er det desværre ikke hensigtsmæssigt. For det første findes 100% sikre edb-baserede systemer ikke. Det er en realitet vi må leve med. Spørgsmålet om risikoen ved et bestemt edb-baseret system er derfor altid relevant. For det andet er det praktisk umuligt at definere kvalitetsegenskaberne, så man entydigt kan sætte procent på sikkerheden. For det tredje findes der kun målemetoder til evaluering af nogle kvalitetsegenskaber. For det fjerde er absolut sikkerhed ikke et mål i sig selv. Normalt tilstræbes et passende sikkerhedsniveau for et givent system. De tekniske løsninger, der vælges, må afpasses såvel menneskelige som økonomiske faktorer og ikke pålægge uacceptable eller upraktiske sikkerhedsforanstaltninger.

I vejledninger til standarden IS9126 arbejdes med sikkerhedsniveauer, som bl.a. fastlægges ved de teknikker, som anvendes til at evaluere egenskaben. Der arbejdes med fire niveauer: A til D, hvor A er det højeste. På baggrund af de anvendelser, som er

analyseret i afsnit 6, må det krævede sikkerhedsniveau være mindst B. Der er tale om kritiske data og anvendelser. Det betyder, der må etableres sikkerhedsforanstaltninger, som giver en meget høj grad af sikkerhed og der må kræves relativt formelle teknikker til at evaluere om sikkerheden er opnået.

b) Scenarier

I denne verden opereres med trusler, dvs. handlinger, som kan betyde et brud på de tre nævnte sikkerhedsformål, og sikkerhedsforanstaltninger, som anses for passende svar på truslen.

Nedenfor belyses sikkerhedsspørgsmål med udgangspunkt i en række hændelser, som fører til et "trussel-scenario". Grundlaget for disse scenarier er, at borger ic-kortet benyttes til en række af de anvendelser, som er behandlet i afsnit 4.

1. Kortet modtages af en forkert person ved udsendelsen/udleveringen .

Når man først er i besiddelse af et borger ic-kort og evt. har kortindehaver-identifikationen, må det antages, at det giver meget vide muligheder. Modtagelse af en anden persons kort giver mulighed for misbrug.

Følgende sikkerhedsforanstaltninger bør iværksættes:

Der må etableres en meget omhyggelig procedure for udlevering af kortet.

Ved produktionen af kortet indbygges en entydig identifikation af kortet (en såkaldt hallmark key). Der skal ske en registrering af kortets identifikation i et centralt register. Ved denne registrering sikres bl.a., at en person ikke kan få udleveret to kort.

Dernæst skal kortet opstartes med de oplysninger, man har besluttet der skal findes i kortet, f.eks. cpr-nr, navn og adresse og forskellige data. Hvis personbeviset indeholder et krypteringsnøgle-par, skal dette dannes og den offentlige nøgle registreres hos nøglecenteret. Endelig - og meget vigtigt - skal der lagres oplysninger, som benyttes til at foretage kortindehaver-identifikationen.

Ved udleveringen skal personen identificeres. Det vil være et bidrag til sikkerheden ved udleveringen, at kortet er forsynet med foto. Ved udskiftning af kortet - der må forventes at skulle foretages ca. hver 10. år - vil der ske en kopiering af kort-indholdet, og kortets procedure til kortindehaver-identifikationen kunne anvendes til identifikationen.

Det må vurderes, at der ikke kan opnås tilstrækkelig sikkerhed ved udsendelse af kortene med posten. Personbeviset bør derfor udleveres af kort-udsteder, hvor man kan sikre en meget stor troværdighed for

- at personbeviset udleveres til den rigtige person,
- at data, der indlægges på kortet er korrekte,
- at der ikke sker en registrering af data, som kun skal findes i kortet.

2. Uvedkommende skaffer sig et kort og vil læse indholdet

Det er et afgørende krav til sikkerheden, at kortets data ikke må kunne læses af uvedkommende.

Den første sikkerhedsforanstaltning er, at kortet produceres "tamper resistent". Dette betyder at man ikke (med realistisk økonomisk og teknisk indsats) kan trænge ind i det på illegal vis. Forsøges dette slettes simpelthen alt indhold.

Den næste sikkerhedsforanstaltning er en kortindehaver-identifikation. Det vil sige, at for at kunne bruge kortet, skal man afgive en korrekt kode. Et forslag til kortindehaver-identifikation er nærmere beskrevet nedenfor i afsnit d.

Såfremt der angives forkert kendeord tre gange, låses kortet, og det kan ikke bruges.

3. Kortet anvendes af uvedkommende, som har skaffet sig adgang til tal-koden

Tal-koden kan komme til andres kendskab, enten ved at den ikke er opbevaret betryggende (bliver stjålet fordi den er skrevet ned) eller ved sløseri (bliver oplyst til andre).

Sikkerheden omfatter også kort-indehaveren, som er ansvarlig for at hemmeligholde sin talkode. Det vil være vigtigt med tilstrækkelig og forståelig information herom. Det må derfor anses for væsentligt, at talkoden er selvvalgt - og at det anbefales, at

denne ikke må skrives ned, men skal huskes og aldrig overdrages til andre.

En række sikkerhedsforanstaltninger kan ikke afvise truslen, men være modtræk.

Et første tiltag er at have foto på kortet. Dette vil kunne afsløre forsøg på misbrug i visse situationer.

Kortets særlig hallmark-key er registreret i et centralt register. Når kortet mistes, kan det derfor spærres i dette register. Ved visse anvendelser bør der ske kontrol heraf, og misbrug vil kunne afsløres.

Det foreslås nedenfor, at der arbejdes med to koder, dels en otte-cifret tal-kode og dels en biokode (f.eks. fingermønster). Ved at benytte biokoden til kortindehaver-identifikation vil man kunne udelukke, at talkoden er kommet uvedkommende til kendskab. Man kan derfor stille krav om denne identifikations-måde ved kritiske anvendelser.

4. Borger ic-kortet kan ikke bruges, fordi personen har glemt sin kode

Hvis man anvender både biokode og tal-kode, vil kortindehaveren kunne henvende sig til kort-udsteder og her indlægge en ny talkode efter at have identificeret sig med biokoden.

Hvis man kun anvender en talkode, vil man uundgåelig stå over for en meget vanskelig procedure. Man kunne tillade, at man hos kort-udsteder har mulighed for at "åbne" kortet og indlægge en ny tal-kode efter en meget sikker identifikations-procedure. Men dette er udfra en sikkerhedsbetragtning problematisk. I denne procedure vil et foto på kortet være et bidrag til sikkerheden.

Set fra et sikkerheds-synspunkt skal proceduren være besværlig for at modvirke sløseri. Det må vurderes, at man er nødt til at kunne gennemføre en sådan procedure, hvis tabet af data på kortet er meget alvorligt, f.eks. hvis der opbevares en privat krypteringsnøgle. Og som konsekvens heraf må det anbefales, at der også anvendes en bio-kode.

5. Kortet går i stykker eller mistes: hvordan får personen et nyt borger ic-kort?

Ved 4 mill. kort vil der selvfølgelig løbende være kort, som ikke virker. Kort kan desuden gå i stykker eller mistes.

Der er ikke noget principielt problem i at udstede et nyt borger ic-kort efter proceduren for udlevering og med en spærrings-markering i det centrale register af det gamle kort. Sikkerhedsproblemet handler om, hvordan det undgås, at data går tabt.

Databærer

Hvis borger ic-kortet anvendes som databærer, er der et umiddelbart behov for at kunne reetablere de data, der var på kortet. Den velkendte sikkerhedsforanstaltning er backup, dvs., at man foretager en sikkerhedskopiering af dataene, så de kan genindlægges på et nyt kort.

En backup procedure kan tilrettelægges på to måder:

- Det er borgeren, der er ansvarlig for backup af sit kort og selv gennemfører den. Denne backup må foregå på udstyr, som den enkelte har i hjemmet, dvs. en kortlæser, en pc og et (godkendt) backup-program. Sikkerhedskopien kan læses over på et backup-

kort eller lagres på et andet medie (harddisk, diskette). Om der er behov for flere generations-kopier er et åbent spørgsmål. En sådan procedure vil kunne tilrettelægges, men man kan næppe regne med, at den vil blive anvendt generelt. For data, som er af stor betydning for kort-indehaveren, er der selvfølgelig større chancer for, at der vil blive foretaget backup i takt med ændringer af dataene.

- I forbindelse med at data indlægges på kortet eller læses af en offentlig bruger, registreres dataene i et centralt backup-register. En sådan procedure vil også kunne tilrettelægges, men den har også minusser: den er omkostningskrævende og er næppe ønskværdig ud fra persondata-beskyttelseshensyn.

Kan der ikke etableres en pålidelig backup er alternativet (supplementet) genindlægning af data. Dataene kan hentes fra personens egne papir-arkiver, eller de kan være opbevaret i edb-registre de steder, der oprindelig har lagt dem ind på kortet. Dataene kan herefter indlægges på et nyt kort, der har en initieringsdato. Ved anvendelser, hvor sådanne data benyttes skal der være adgang til denne dato og der må kunne tages højde for, at der er tale om et nyt kort, hvor data kan mangle eller være ufuldstændige.

Det må vurderes, at det er muligt at etablere sikkerhedsforanstaltninger over for datatab, hvis kortet mistes. Men disse

sikkerhedsforanstaltninger er hverken enkle eller meget sikre, og man kan ikke regne med at undgå datatab. Dette problem er voksende, hvis der opbevares store datamængder og hvis de opbevares over en lang periode, f.eks. efter dataene er slettet i de offentlige edb-registre.

Digital signatur

Opbevares et krypteringsnøgle-par til en digital underskrift på kortet, er det helt afgørende, at den private nøgle ikke mistes, da dokumentations-muligheden for foretagne underskrifter forsvinder. Den private, hemmelige nøgle skal principielt kun findes på borger ic-kortet. Den offentlige nøgle udgør ikke et problem, da den findes hos nøglecenteret.

Backup-procedurer, som omtalt ovenfor, må afvises, da de indebærer en uacceptabel risiko for, at den private nøgle kan blive afsløret.

I stedet kan der ved udstedelse af borger ic-kortet samtidig udarbejdes en kopi, som indeholder samme sikkerhed som det egentlige personbevis, men herudover kun identifikation, den private hemmelige nøgle og evt. andre tilsvarende oplysninger. Kopien kunne opbevares af personen, men det må vurderes, at det ikke giver tilstrækkelig sikkerhed for, at kopi-kortet er til stede, når der er behov. Det må derfor anbefales at kopi-kortet opbevares af kort-udsteder.

Ved udlevering af et nyt kort skal det ved en særlig procedure hos kort-udsteder være muligt at overføre den private, hemmelige nøgle fra kopi-kortet til det ny kort. Ved denne kopiering er der den trussel, at nøglen læses. Den må derfor krypteres med en nøgle, som kun findes i det modtagende ny kort. Proceduren er iøvrigt også nødvendig, når borger ic-kortet skal udskiftes pga. alder.

6. Kortet indeholder forskellige følsomme personlige oplysninger og ved henvendelse på Arbejdsformidlingen får konsulenten adgang til helbredsoplysninger.

Det første sikkerhedstiltag er, at de kort-læsere, der kan anvendes til at læse kortet skal autenticeres over for kortet. Dvs. kun kort-læsere, som er knyttet til systemet, kan anvendes.

En given bruger bør selvfølgelig kun have adgang til de data, som er relevante. Inden for én sektor kan der også være tale om, at forskelligt personale kun skal have adgang til begrænsede dele af kortets data. Spørgsmålet her er, om der kan etableres en tilfredsstillende adgangskontrol [48].

Adgangskontrollen har to led:

- at *kortindehaveren* giver tilladelse til, at en bruger får adgang til kortet og til bestemte data,

2) at der *i kortet* foretages en kontrol af brugerens adgangs-rettigheder.

Kortindehaverens kontrol

Adgangs-kontrollen kan som første led styres af kort-indehaveren. Efter kortindehaver-identifikationen kan han give tilladelse til, at en bruger får adgang til bestemte data på kortet. Først herefter har brugeren mulighed for at læse data fra kortet. Brugeren (der også kan være en computer) får således adgang til bestemte data på kortet gennem en åbnings-dialog mellem kortindehaver og kortlæser.

Man kan dog tænke sig, at der defineres særlige bruger-password, som giver én nærmere fastlagte rettigheder uden kortholders identifikation (f.eks. til helbredsoplysninger der er relevante ved akut behandling).

Bruger-adgangskontrol

I en række anvendelser bør kortindehaver-kontrollen suppleres med adgangskontrol for brugeren.

Det er teknisk muligt helt at adskille de enkelte data-filer i kortet og give hver enkelt sit eget password.

Brugeren skal over for kortet kunne afgive et password, som kortet kan kontrollere giver rettigheder til de ønskede data. Det centrale sikkerhedsspørgsmål er at sikre, at disse passwords ikke spredes til uvedkommende. En mulighed er, at det opbevares på

et kort eller lignende, som brugeren har, og indlæses herfra, når terminalen åbnes. En anden mulighed er, at password'et ligger i terminalen og at brugeren skal kunne identificere sig over for terminalen for at få adgang.

Kortindehaveren bør have adgang til data på sit eget personbevis. Der bør således ved kort-indehavers identifikation samtidig gives rettigheder til selv at læse/skrive/ændre data på kortet.

7. Når kortet anbringes i terminalen bliver kendeord og andre oplysninger tappet

Det er afgørende for systemets troværdighed, at man kan være sikker på, at oplysninger man afgiver i en kommunikation ikke bliver registreret af andre. Specielt må man være sikker på, at tal- og biokode ikke tappes.

Det er teknisk muligt at bygge kort-læsere som en tamper-resistent enhed, dvs. en enhed, der (inden for realistiske praktiske og økonomiske grænser) bl.a. ikke kan tappes for oplysninger.

Når data forlader kort-læseren og kommunikeres til et edb-system, kan der være en risiko for at dataene kan tappes. Sikkerhedsforanstaltningen over for den trussel er kryptering af dataene.

8. I forbindelse med brug af kortet giver borgeren udtryk for at oplysningerne på kortet eller i edb-systemet er forkerte: "De må være rettet eller indtastet forkert"

Det er en del af sikkerheden ved edb-systemet, at data i systemet, herunder data, der er indlæst i kortet, er korrekte. Men hvilke muligheder har kort-indehaveren for at dokumentere sin opfattelse?

En mulighed er, at der til de enkelte oplysninger knyttes en digital underskrift, så man altid kan kontrollere, hvem der har indlagt oplysningerne. Noget tilsvarende kan knyttes til de oplysninger kort-indehaveren har afgivet.

For andre anvendelser kan der i kortet dannes en log-fil, som registrerer anvendelse af kortet. Opstår der senere tvivl, kan logfilen udskrives og benyttes til dokumentation.

c) kortet

Ic-kort teknologien giver langt bedre mulighed for et højt sikkerhedsniveau end tidligere plastkort, f.eks. magnetstribe-kortet. Ic-kortets evne til at behandle data giver en række muligheder for at forbedre sikkerheden. Hvor magnetstribe-kortets sikkerhed er snævert knyttet til on-line kommunikation med et edb-system, kan der etableres sikkerhed med ic-kortet i off-line systemer.

Et ic-kort anses for en tamper-resistent enhed, dvs. hemmeligholdelsen af indholdet i kortet kan ikke brydes. Det er ikke praktisk muligt at producere falske kort og det er ikke muligt at tappe datakommunikation i kortet. De data i kortet, som ønskes holdt fortrolige eller hemmelige krypteres, så de ikke kan læses uden korrekt kortindehaver-identifikation.

Det er muligt at danne en log-fil i kortet, som registrerer kortets anvendelser og kan bruges til dokumentation i tvivlstilfælde. Log-filen kan dannes som en cyklisk fil, således at registreringerne slettes, når maximum antallet er nået. Log-filen er en "read-only" fil for kortindehaveren.

Det er centralt for et borger-kortsystem, at kortet er meget pålideligt. Hvis anvendelsen af kortet i kommunikationen mellem borgeren og de offentlige myndigheder bliver almindelig, vil det være en forudsætning, at kortet virker nærmest hver gang. Det er oplyst, at ic-kort kan leveres med en garanteret levetid på 10 år med en meget beskeden fejlpromille.

d) Kortindehaver-identifikation

Et helt central sikkerhedselement er kortindehaverens identifikation før kortet anvendes. Proceduren skal sikre, at det er kortets indehaver, som vil benytte kortet, og altså på den anden side være opbygget så uvedkommende, der f.eks. har stjålet kortet, ikke kan anvende det. Kortindehaver-identifikationen er et afgørende punkt, hvor kortindehaveren indgår som aktør i tilvejebringelse af sikkerhed i kort-systemet.

Et velkendt eksempel er brug af Dankortet, hvor der skal indtastes en PIN-kode, et fire-cifret tal, som bliver kontrolleret, før kortet kan anvendes. Et andet eksempel er indtastning af et password eller kendeord, der typisk er 6 bogstaver og andre karakterer, før man får adgang til edb-systemet på sit arbejde.

Kortindehaver-identifikationen er et afgørende og ofte svagt led i sikkerheden, fordi kortet er åbent, hvis koden kendes af uvedkommende.

Da ic-kortet kan databehandle, har det særlige muligheder for en sikker procedure til kortindehaver-identifikation. Verifikationen kan ske i kortet og det kan indeholde særlige oplysninger, som kan benyttes til identifikationen. Disse oplysninger kan beskyttes mod uvedkommende ved kryptering.

Det skal her foreslås, at der anvendes to kortindehaver-identifikationer:

- en tal-kode og
- en bio-kode.

Tal-koden er velkendt fra PIN-koderne og kan indføres ganske enkelt. Biokoden er en talværdi, der er beregnet på grundlag af et biometrisk kendetegn ved personen.

To koder

Når der anbefales to koder, skyldes det ønsket om at indføre anvendelse af en biokode. Med en biokode kan der skabes en høj grad af sikkerhed ved anvendelse af kortet.

På den anden side vurderes det, at et borger ic-kort ikke alene kan have bio-koden som kort-indehaver-identifikation. Anvendelse af bio-koden medfører en fordyrelse af kort-læseren og man kan ikke forvente den kan benyttes alle steder af praktiske og økonomiske grunde. F.eks. vil det ved kortlæsere, der anvendes i hjemmet, være en urimelig fordyrelse.

Videre må det skønnes, at der er en del af befolkningen, som ikke ønsker at benytte en bio-kode af private grunde. En del af befolkningen vil endog af fysiske grunde været afskåret fra at anvende biokoden. Det må derfor vurderes som hensigtsmæssigt, at der er frivillighed - medmindre anvendelsen klart taler for bio-koden. Omvendt skal man være opmærksom på at en gruppe i befolkningen ikke kan anvende en tal-kode, men får mulighed for at benytte kortet ved at bruge bio-koden.

Fordelene ved at have bio-koden ligger i den høje grad af sikkerhed. Ved anvendelser, der vurderes at kræve høj sikkerhed, kan man kræve anvendt bio-koden til identifikation. Som det er belyst i scenarierne ovenfor, kan man anvende bio-koden når kortet mistes, skal udskiftes, tal-koden er glemt osv.

Tal-kode

Den almindeligste måde til kortindehaver-identifikation er anvendelse af en tal-kode (PIN, personal identification number), der typisk er et tal på fire cifre.

Ved anvendelse af ic-kort sker kontrollen af, om den angivne tal-kode er korrekt, ved en databehandling i kortets computer. Tal-koden findes altså kun i kortet og opbevares her krypteret i kortets hemmelige dataområde.

Et grundlæggende problem med PIN-koden er, at kortindehaveren skal *huske* koden. Det foreslås at tal-koden er selvvalgt og kan ændres af kortindehaveren ved besøg hos kort-udsteder. Hermed er det muligt at lave tal-koder, som kan huskes memoteknisk ved at knytte tallene til noget man kan huske. Et forslag er dagen i datoen på et antal fødselsdage. Et kendt problem med selvvalgte tal-koder er, at de laves, så de er lette at gætte. Det skal derfor anbefales at tal-koden bliver på 8-cifre.

Det må samtidig meget kraftigt anbefales, at man ikke *opbevarer* sin tal-kode. Det skal bemærkes, at en anvendelse af personbeviset er at sikre, at man kun skal huske denne ene tal-kode.

Biokode

Man kan aflæse og give et digitaliseret billede af mange kendetegn ved personen, f.eks.: underskrift, fingeraftryk, blodåre i håndfladen, stemmegenkendelse, blodårer i øjet, striber i iris, håndformen [49]

Den traditionelle fremgangsmåde har været at lagre det digitaliserede billede i kortet, og når kortindehaver-identifikationen skal gennemføres at aflæse billedet igen og sammenholde det med kortets data og på den måde verificere, at det er kortindehaveren som vil benytte kortet.

Med en biokode er det *ikke* det digitaliserede billede, som opbevares, men kun en deloplysning eller en beregnet talværdi, som gør det muligt at gå fra det digitaliserede billede til talværdien. *Men ikke omvendt*. Den lagrede bio-kode kan altså ikke bruges til at identificere personer. Bio-koden findes kun i kortet, lagret i et hemmeligt område, der ikke er tilgængeligt. Identifikationen er

så at sige udelukkende en sag mellem personen og hans eget borger ic-kort.

Et eksempel er en biokode på grundlag af fingeraftrykket: et *fingermønster*.

Aftryk af en finger udgør en entydig identifikation af kortindehaveren. Med et finger-mønster anvendes kun et antal punkter i fingeraftrykket. Antallet afhænger af den krævede sikkerhed, men 8 punkter skulle give en sikkerhed mindst på niveau med en tal-kode på otte cifre. Finger-mønsteret lagres kun i kortet i dets hemmelige område, der ikke er tilgængeligt. Finger-mønsteret udgør en digital repræsentation, som kan sammenlignes med et scannet billedet af fingeraftrykket. Det er vigtigt at bemærke, at det kun er én-vejs. Man kan kun gå fra det scannede fingeraftryk til det lagrede finger-mønster, men ikke fra finger-mønsteret til et finger-aftryk. Man kan øge sikkerheden, for at kortindehaveren ikke bliver afvist, ved at indlægge fingermønster for to fingre fra hver sin hånd ind i kortet. Der kan så prøves med en ny finger, hvis den første f.eks. har fået skrammer, og derfor ikke godkendes.

Fingeraftrykslæseren kan fungere på den måde, at man bevæger fingeren henover en glasplade. Under glasplade sidder en læser, der scanner fingeren linje for linje og omsætter det til et digitaliseret billede. Fingerscanneren kan afgøre, om det er en levende finger, der aflæses eller om der er tale om falsk efterligning.

Et andet eksempel er en biokode på grundlag af *underskriften*.

Kortindehaveren "skriver" sin underskrift med en særlig pen. Pennen viser ikke underskriften, men måler acceleration, drejninger og tryk. Disse værdier kan sammenholdes med værdier for underskriften gemt i kortet. Man kan således ikke lave underskriften på grundlag af de værdier, der er gemt i kortet. I kortet opbevares værdier fra flere underskrifter, og nogle af disse udskiftes i takt med ændringer i underskriften.

En tredje eksempel er en biokode på grundlag af blodårer på bagsiden af hånden: *venecheck*.

Der foretages en infrarød scanning af hånden og ud fra blodårernes placering (veins and position of bloodvessels) skabes et digitaliseret billede, som beregnes til en 16- eller 8-cifret talværdi. Det digitaliserede billede slettes straks og kun biokoden opbevares på kortet. På den måde opnår man den centrale karakteristik ved biokoden, at man kan gennemføre kortindehaver-identifikationen, men at man ikke kan identificere personen ud fra biokoden.

Anvendelse af biokoder er en ny teknik, der er gået fra eksperiment-fase til praktisk anvendelse, men endnu ikke anvendes i større systemer.

e) Kortlæser

Sikkerhedskravene til kortlæserne handler om:

- beskyttelse mod aflytning under indtastning og databehandling,
- beskyttelse mod afsløring af data ved fysisk indtrængen i kortlæseren.

Til Dankort-systemet blev der udviklet et særligt sikkerhedsmodul som opfyldte disse krav, og som kunne kryptere og dekryptere data i forbindelse med data-kommunikationen. Det må forventes, at der tilsvarende vil kunne udbydes prisbillige kortlæsere med høj sikkerhed til ic-kort.

Det skal tilføjes, at der ikke i alle sammenhænge vil være behov for kortlæsere med dette sikkerhedsniveau. F.eks. vil kortlæsere i hjemmet, der enten er fritstående eller indbygget i pc'en, ikke kræve disse sikkerhedsforanstaltninger.

f) Datakommunikation

Der gennemføres normalt en række sikkerhedsforanstaltninger for at sikre datakommunikationen således, at de data, der transmitteres, kommer frem, at de modtagne dataelementer faktisk hører til dataudvekslingen og at dataene er korrekte og uændrede.

En af sikkerhedsforanstaltningerne er kryptering af dataene. I nogle anvendelser vil kryptering af dataene kunne ske i borger ic-kortet. I andre anvendelser, hvor kort-læseren hører til et bestemt edb-system, vil krypteringen ske i kort-læseren. For disse anvendelser vil der også blive gennemført en procedure, som skal sikre at den benyttede kortlæser, der benyttes tilhører systemet og er autoriseret.

Datakommunikationen fra kort-læseren til edb-systemet, enten det er et lokalt eller et centralt system, er en grænseflade mellem

kortsystemet og edb-systemet. Sikkerhedsspørgsmål vil hovedsageligt blive afklaret i sammenhæng med edb-systemet.

[48] Gunnar Klein: Intermittently Connected Devices Security Requirements CEN TC224/WG7

[49] BTT: Biometric Templates: Size no longer a factor? i Biometric Technology Today july/august 1993.
John McCrindle: Smart Cards () John R. Parks: Automated Personal Identification Methods for Use with Smart Cards. I: P.L.Hawkes, D.W.Davies and W.L. Price: Integrated Circuit Cards, Tags and Tokens (1990)

6. Brugbarhed

I dette afsnit opstilles krav til brugbarheden i et kort-system og dernæst behandles nogle centrale problemer med relation til brugbarheden.

Med brugbarhed tages der udgangspunkt i brugeren af kort-systemet. Med brugeren menes her i dette afsnit kort-indehaveren. Brugbarhed handler om hvordan det er at bruge borger ic-kortet og kort-systemet. Er det rart at bruge? Hvis alle voksne får et borgerkort, er det af afgørende betydning, at kortet har en "høj brugbarhed".

Med brugbarhed menes at systemet:

- er let at lære og let at huske, hvilket kan måles med den tid, det tager at lære at løse bestemte opgaver og den tid det tager for en bruger, der har været væk fra systemet en vis tid, at løse opgaven igen,
- er effektivt at bruge, hvilket kan måles som hastigheden, hvormed bestemte opgaver løses af bruger og system i forening

- er tilfredsstillende at bruge, hvilket er udtryk for brugerens subjektive tilfredshed med systemet [50].

a) Kvalitetskrav

Med kvalitet menes her kort-systemets "egenskaber og karakteristiske træk - set som helhed - som har noget at gøre med dets evne til at opfylde specificerede eller underforståede behov" (DS/ISO 8402: Kvalitet - ordliste). Ved edb-systemer (software) forsøges kvaliteten specificeret med en række egenskaber. ISO-standarden, "Information technology - software product evaluation" definerer en række "software quality characteristics" (kvalitetsegenskaber) og i et bilag forslag til uddybende "sub-characteristics" (IS9126).

Kvalitets-egenskaben brugbarhed (usability) angiver indsatsen for at bruge systemet og den individuelle vurdering af denne brug. Egenskaben brugbarhed uddybes med tre sub-characteristics:

- forståelse (understandability), der angiver indsatsen for at forstå systemets logiske begreber og anvendelse,
- indlæring (learnability), der angiver indsatsen for at lære at anvende systemet,
- betjening (operability), der angiver indsatsen for at kunne kontrollere betjeningen af systemet.

Et borgerkort skal i princippet kunne anvendes af alle. Der må derfor stilles krav til brugbarheden, som afspejler dette krav. Et eksempel på et måleligt kvalitetskrav for en anvendelse kunne være:

- af 100 tilfældige danskere skal de 99 kunne bruge pågældende anvendelse inden for 5 minutter på baggrund af en kort vejledning,

og videre

- på baggrund af brug af en anvendelse over 3 uger skal gennemsnitsopfattelsen være "meget tilfreds" og ingen må angive "helt utilfreds".

Det må kræves, at kort-udsteder dokumenterer kort-systemets høje brugbarhed. Det må ske dels ved en dokumentation for, at standarder for bruger-grænsefladen overholdes, og dels ved at der gennemføres forsøg/test af brugbarheden. I vejledninger til IS9126 angives kvaliteten i fire niveauer fra A til D, hvor A er det højeste niveau. De krav der stilles her betyder at borger kort-systemet vil skulle opfylde krav til niveau B.

b) Kunne bruges af alle

Når vi siger, at borgerkort-systemet skal kunne bruges af alle, er det nødvendigt at skelne mellem udsagnet, som en kvalitets-egenskab og som et overordnet mål for borger ic-kortet.

Ser vi på den kvalitets-egenskab, at borger ic-kortet kan bruges af alle, må der tilføjes: *som ønsker at anvende det*. Det er et krav til brugbarheden, at alle der ønsker at anvende kort-systemet kan gøre det.

At alle faktisk bruger borger ic-kortet er et mål for borgerkortet. Forskellige holdninger til at bruge edb i almindelighed og plastkort i særdeleshed må respekteres, men en gennemtænkt og afprøvet brugergrænseflade må antages at bidrage til, at flest muligt ønsker at bruge borger ic-kortet som led i en eller flere anvendelser.

Brugerne eller kort-indehaverne er ikke en ensartet masse af mennesker. I bruger-analyser beskrives brugerne på baggrund af viden og erfaring, uddannelse og træning, fysiske og cognitive attributter [51]. En beskrivelse af den danske befolkning på dette grundlag vil give et meget varieret billede. Måske er der ikke to helt ens brugere?

Udgangspunktet er, at der ikke kan stilles nogen krav til forudgående brugerviden eller uddannelse. Tværtimod skal borgerkort-systemet kunne bruges uden vejledning eller på grundlag af en enkel vejledning. I et borger ic-kort med en række forskellige anvendelser vil omfanget af den vejledning, som kan accepteres, være afhængig af den enkelte anvendelse. Benyttes borger ic-kortet f.eks. til erstatning for Dankortet, skal det kunne anvendes uden vejledning, mens der ved en anvendelse, som brevhemmelighed må accepteres en mere omfattende vejledning.

For at sikre en høj brugbarhed må det være et krav til kort-systemet, at brugergrænsefladen må være ensartet i hele systemet. Uanset om kortindehaveren står i banken, sidder hos lægen eller hjemme ved sin egen pc, skal betjeningen af kort-systemet ske på samme måde.

I et borger kort-system må der tages hensyn til forskellige handicaps, som kan gøre det vanskeligere at benytte borger ic-kortet [52]. Det har ikke indgået i udredningen at undersøge dette spørgsmål nærmere. Men der kan peges på, at sådanne overvejelser bør spille en særlig rolle i valget af kortindehaver-identifikation, da den er forudsætningen for overhovedet at bruge kortet. Det vil næppe være muligt at sikre, at alle med fysiske handicap kan benytte systemet alle steder, men det bør være muligt at sikre, at alle kan bruge det nogle steder.

c) Valg af anvendelse og data

Med et multifunktions-kort opstår et nyt problem ved anvendelsen af plastkort, nemlig at kort-indehaveren skal styre, at det er den rigtige anvendelse og de rigtige data, som benyttes.

Vil kortindehaveren benytte kortet som Dankort, skal hun først angive, at det er denne anvendelse, som skal benyttes, og derefter skal hun udvælge den rigtige bruger-identifikation, dvs. konto og pin-koder eller en anden identifikation, som hun har i sit kort. Dialogen skal udbygges med et trin ud over de, vi kender fra brug af Dankort.

Er kortindehaveren på apoteket og skal overføre sin recept skal han først angive, at det er anvendelsen bærer af recepter, som skal bruges, og derefter vælge den recept apoteket skal have.

I modsætning til de plastkort vi kender i dag, skal der etableres en dialog mellem kortindehaveren og udstyret (kortlæser, en terminal, en pc) om valg af anvendelse og data.

Valget af funktion på kortet kan dog i en række tilfælde helt eller delvist automatiseres. Når kortlæseren hører til et bestemt edb-system kan kommunikation mellem kortet og kortlæseren definere, hvilken tjeneste på kortet, der skal benyttes. Anbringes borger ic-kortet i en kontant-automat, kan en dialog mellem automaten og kortet afgøre, at der skal sendes en bruger-identifikation fra kortet og evt. kan kortet finde de bruger-identifikationer, der kan anvnedes i en kontant-automat så kort-indehaveren kun skal vælge blandt disse. Som i alle gode dialog-systemer skal der være genveje og kort-indehaveren skal have mulighed for straks at angive hvilken bruger-identifikation (pin-kode mv.), der skal benyttes.

I del 10 om dialogprincipper af ISO-standarden 9241 [53] fastsættes, at et dialogsystem i almindelighed kan siges at være velegnet, hvis det lever op til følgende syv principper:

- hensigtsmæssigt for opgaven,
- selvbeskrivende,
- kontrollerbar,

- svare til brugerens forventninger,
- fejltolerant,
- egnet for individualisering,
- egnet for indlæring.

I standarden uddybes disse principper. Her skal blot konstateres, at det må vurderes som realistisk at konstruere en brugergrænseflade, så brugeren let og effektivt kan vælge anvendelse og data på borger ic-kortet.

d) Forstå anvendelsen

En del-egenskab ved "brugbar" er brugerens forståelse af systemet. Kort-indehaveren skal både kunnne overskue, hvad der sker når borger ic-kortet benyttes og desuden kunne kontrollere anvendelsen. En sådan forståelse vil være et element i kort-indehaverens subjektive tilfredshed med kort-systemet.

Blandt en række forbrugerpolitiske vurderings-kriterier til betalingskort opstillede man kriteriumt:

- Systemets kompleksitet må tilpasses forbrugernes informationsniveau [54].

"Primært må vurderings-kriteriumt derfor defineres som kravet om enkelhed og gennemskuelighed: Kompleksiteten skal møde brugerne på deres informationsniveau. Sekundært må det forlanges, at på de områder, hvor systemet i sin natur ikke kan gøres selvforklarende, må der stilles så omfattende information til forbrugerens rådighed, at hans informationsniveau bringes på højde med det, systemets kompleksitet kræver" (s. 186). Denne balance mellem systemets kompleksitet og kort-indehaverens informationsniveau er også relevant for et borger ic-kort. For en række anvendelser vil det primære krav om enkelhed kunne opfyldes. For andre vil kravet om tilstrækkelig information kunne opfyldes, men for nogle anvendelser kan der forudses problemer.

Som eksempel kan nævnes anvendelsen digital signatur. En underskrift er noget meget personligt og privat, og det er sin sag at lade den overtage af en elektronisk databehandling, som er mere eller mindre uforståelig. Det fremgår af behandlingen af digital signatur i afsnit 4.B og tillægget om kryptering i afsnit 4.C, at det er vanskeligt at forstå, hvordan en digital signatur fungerer. Og inddrager vi den bagvedliggende matematik, er det helt uforståeligt for de allerfleste. Men hvor meget skal vi forstå for at acceptere at bruge den digitale signatur?

I dagens samfund bruger vi alle masser af teknik, hvis nærmere måde at fungere på vi ikke forstår. De er så at sige en sort kasse, som dog gør noget forudsigeligt, når vi bruger dem. På samme måde kan vi acceptere den digitale signatur som en teknik, der giver et forudsigeligt resultat, når vi anvender den.

Information er ikke blot generel skriftlig vejledning om digital signatur, men generelt en brugergrænseflade, som giver kort-indehaveren kontrol med udfærdigelse af sin digitale signatur. Her kan bl.a. indgå:

- en dialog, som gør det helt klart hvilket brev eller dokument, der underskrives,
- et system, der automatisk gemmer brevet i et arkiv og har en brugervenlig arkiv-håndtering,
- en udskrift, hvor underskriften er vist som tal og bogstaver og knyttet til brevet/dokumentet, som også kan danne grundlag for en visuel sammenligning med modtagerens papirkopi.

Desværre vil et system som laver en digital signatur være komplekst, så der er ikke anden mulighed end at gøre anvendelsen så enkel og gennemskuelig, at der opnås en tilfredsstillende subjektiv brugertilfredshed.

[50] Baseret på Rolf Molich (red): Brugervenlige edb-systemer (1986).

[51] Her hentet fra udkast til del 11: Guidance on usability specification and measures af ISO-standarden 9241: Ergonomic Requirements for office-work with visual display terminals (VDT's).

[52] Jfr. den amerikanske lov fra 1990: Americans with Disabilities Act. "Loven skal være med til at sikre at de cirka 43 millioner amerikanere med en eller anden form for handicap ikke diskrimineres hverken på arbejde eller i fritiden". Hans Kyster: Menneske-Maskin-Samspil (1993) s. 33.

[53] ISO standard 9241 op.cit. Del 10 Dialogue Principles. Omtalt i Hans Kyster op.cit. s. 75-80.

[54] Preben Sander Kristensen og Folke Ölander: Forbrugerpolitiske aspekter ved elektronisk betalingsfor midling med købekort s. 186-198. I: Betænkning 965 (1982)

7. Vurdering

I dette afsnit fremlægges en vurdering af brug af ic-kort til borgerkort. Vurderingen bygger videre på de analyser der er foretaget i afsnit 6 af anvendelses-eksemplerne. Dernæst forudsætter vurderingen, at de kvalitetskrav og løsninger, der er behandlet i afsnit 5 om sikkerhed og afsnit 6 om brugbarhed, opfyldes. Medmindre der fremlægges overvejelser herom, som har konsekvenser for den samlede vurdering.

Vurderingen gennemføres i to tempi. Først foretages en funktionel vurdering, som besvarer spørgsmålet om hvad der er teknisk muligt og hensigtsmæssigt. Dernæst behandles resultatet af denne vurdering i de følgende to afsnit, som uden egentlig konklusion, lægger op til debat om hvorvidt det fremlagte forslag er en god ide.

7.A Funktionel vurdering

På baggrund af analyserne af anvendelses-eksemplerne kan listes følgende mulige kort-funktioner på borger ic-kortet:

Brugeridentifikation

- nøgle til kommunens egenservice-system,
- opbevaring af pin-koder og anden information, så personbeviset f.eks kan erstatte betalings-kort og disses pin-koder,
- adgangskontrol til edb-systemer, så kortet erstatter/supplerer password,

Digital underskrift

- krypterings-nøglepar, der gør det muligt at afgive en uafviselig digital underskrift,

Brevhemmelighed

- kryptering af data

Registerkontrol

- hemmeligholde (kryptere) personlige data i edb-registre,
- samtykke til videregivelse af personlige oplysninger fra edb-registre,
- identifikation der giver adgang til egne data i edb-registre,

Personlig legitimation

- manuel og automatisk personlig legitimation,
- fysisk adgangskontrol,

Databærer af personlige oplysninger

- stamdata, navn, adresse og personnummer,
- en række helbredsoplysninger (f.eks. kroniske sygdomme, allergier, blodtype, vaccinationer, organdonortilsagn), som kan have betydning i en nødsituation,
- speciel helbredsjournal om en særlig og helbredsmæssig vigtig sygdom hos personen,
- opbevaring af recepter til apotek og oplysninger om aktuelt medicinforbrug,
- vandrejournal i en ledighedsperiode med visse data,

Brugerbetaling

- kreditkort til offentlig service/ydelse,
- betaling bompenge/vejafgifter ved bilkørsel på bestemte veje,
- administration af brugerbetaling.

I afsnit b foretages en samlet funktionel vurdering af disse mulige kort-funktioner. I afsnit c behandles hvilke borger ic-kort, der kan anses for reelle muligheder, og der fremlægges et forslag om et privatkort.

Inden denne vurdering vil det i næste afsnit blive behandlet, i hvilken udstrækning målet om ét kort kan realiseres, og en risikovurdering af gennemførelse af et multifunktionskort.

a) Systemudformning og projektgennemførelse

Et af udredningens udgangspunkter var et mål om, at den enkelte kun skal have ét eller i det mindste få kort ved at udnytte ic-kort teknologiens mulighed for at håndtere en række anvendelser (multifunktionskort) på ét kort.

Med listen over anvendelses-eksempler vil en forudsætning for dette mål være, at borger ic-kortet er et fleksibelt system, som giver mulighed for forskellige anvendelser hos den enkelte borger.

Et sådant koncept, med mange anvendelser og en fleksibilitet i forhold til hvilke kort-funktioner, der er på det enkelte kort, kan beskrives som en *dokument-mappe*.

Af en række grunde må det dog vurderes, at dokument-mappe konceptet ikke kan gennemføres:

Ved udformningen af kortet skal der findes programmel mv. til de kort-funktioner, kortet kan bruges til. Det vil ikke være praktisk muligt på ét ic-kort at samle så mange forskellige anvendelser.

Det må vurderes som sikkerhedsmæssigt uacceptabelt at blande kort-funktioner, der forudsætter brug af adgangskode (tal- eller biokode), med forskelligt sikkerhedsniveau på samme kort.

Endelig må det vurderes, at med fremkomsten af små bærbare edb-maskiner (palmtop computer), findes der teknologiske løsninger, som langt bedre vil kunne anvendes til dokument-mappen. Der er simpelthen ingen fornuft i at ville skabe løsningen i kortformatet. Man taler allerede om den personlig digitale assistent (PDA) som er så lille, at den kan opbevares i lommen eller i tasken. Den kan betjenes med både tastatur og en pen og kan anvendes til kommunikation, f.eks. trådløst som en mobiltelefon. Det falder i øvrigt uden for rammerne af denne udredning at forfølge dette aspekt yderligere.

Selv om dokumentmappe-konceptet må afvises, kan et borger ic-kort indeholde et vist antal kort-funktioner. Et sådan multi-funktionskort har et antal på forhånd fastlagte anvendelser, men det dataindhold, der hører til anvendelsen, f.eks. en pin-kode, kan indlægges senere. Hvor mange forskellige funktioner kortet kan håndtere er afhængig af den enkelte funktions ressourceforbrug (programstørrelse, datalager), men man skal nok ikke forvente over 15 forskellige.

Det må forudsættes, at såfremt en funktion kræver et højt sikkerhedsniveau må alle funktioner have et højt sikkerhedsniveau, således at der ikke er tvivl om betydningen af at hemmeligholde adgangskoden til kortet.

Projektgennemførelse

For at få en nærmere vurdering af mulighederne for at indføre et multifunktions borger ic-kort er der gennemført nogle risikovurderinger med udgangspunkt i SBA-metoden [55] . Det må vurderes, at der er en betydelig risiko ved et multifunktionskort-projekt og på en række områder en stor risiko. Der bør derfor ved en projektetablering bevidst arbejdes på at iværksætte foranstaltninger som mindsker risikoen.

Nogle centrale faktorer for den betydelige risiko ved projektet er:

Selv om man kan sige, at det er teknisk muligt at lave et multifunktions-kort, er teknologien ny og relativ uprøvet. Der skal f.eks. udvikles et operativ-system, som kan styre og adskille de enkelte kort-funktioner.

Det samme må siges om biometriske metoder til kortindehaver-identifikation.

Ic-kortteknologien kendes kun af få folk, som har arbejdet med den. Der er dog en vis erfaring i Danmark, bl.a. som følge af Danmønt-projektet. Desuden har en række kortproducenter og kortsystemleverandører forankring i Danmark. Det må vurderes som afgørende, at de folk, der har erfaring med ic-kort inddrages i/udfører opgaven.

Der er tale om et meget stort projekt, som omfatter udvikling af selve kortet, udvikling af anvendelser hos brugerne, udvikling af udstyr hos brugerne. Projektets størrelse er i sig selv en risikofaktor. Det må i den sammenhæng konstateres, at der næppe er mulighed for først at gennemføre et mindre pilotprojekt.

Projektorganisationen kan blive karakteriseret ved, at der er mange systemejere fra såvel den offentlige som den private sektor. Endvidere kan beslutningerne i betydelig omfang blive politiske beslutningsprocesser. En sådan kombination er erfaringsmæssig meget risikofyldt.

Anvendelsen af borger ic-kortet forudsætter, at der anskaffes udstyr og programmel hos brugerne. Brugerne er såvel offentlige myndigheder som private virksomheder og privatpersoner. Når der i stor skala skal indføres nyt udstyr, er der en risiko for

problemer med at få det til at fungere. Behovet for udstyr hos privatpersoner rejser særlige spørgsmål. Vil udstyret blive anskaffet? Kan det kontrolleres, om det er i overensstemmelse med specifikationer for systemet?

Konstateringen af, at der er en vis risiko for projektgennemførelsen, betyder ikke, at projektet ikke bør gennemføres. Men risikoen for projektet bør føre til en forståelse for, at der må tages særlige initiativer, for at projektet kan gennemføres "til den rigtige tid, til den rigtige pris og med den rigtige kvalitet" (SBA-Projekt).

b) Vurdering af anvendelses-eksemplerne

De vurderinger, der blev foretaget af eksemplerne i afsnit 6, skal her sammenfattes og udbygges til en samlet vurdering af kort-funktionerne ud fra funktionelle betragtninger.

I anvendelses-eksemplet **bruger-identifikation** analyseres tre anvendelser af et borger ic-kort.

Erstatning af Pin-koder på betalingskort o.l. vurderes som en oplagt anvendelse af borger ic-kortet.

Tilsvarende vurderes anvendelse til bruger-identifikation over for kommunalt egenservice system som en oplagt kort-funktion. Og det vil også være tilfældet med andre offentlige og private egenservice systemer.

Endelig vurderes, at borger ic-kortet kan anvendes til adgangskontrol (password) til edb-systemer. Men det understreges, at der er tale om en begrænset anvendelse, da kortet er privat.

Alternative teknologiske løsninger (betalingskort med pin-kode, pin-kode der indtastes, password eller særlige ic-kort) er enten specifikke, væsentlig ringere og/eller ikke eksisterende.

Det kan således sammenfattes, at der her er tale om velbegrundede kort-funktioner, som kan implementeres på et borger ic-kort.

I anvendelses-eksemplerne **digital signatur og brevhemmelighed** analyseres anvendelse af et borger ic-kort til at opnå dokument-sikkerhed, dvs. brevtroværdighed og brevhemmelighed.

Det vurderes i eksemplerne, at der er tale om velbegrundede kort-funktioner, som kan implementeres på et ic-kort.

Der findes konkrete løsninger, dels en løsning hvor nøgler til underskrift opbevares på brugerens pc og er tilgængelig med en pin-kode, dels ic-kort løsninger. Ved anvendelse af et borger ic-kort kan anvendelserne blive bredt tilgængelige og på et højt sikkerhedsniveau.

I anvendelses-eksemplet **registerkontrol** analyseres tre anvendelser, der alle har som overordnet mål at styrke persondata-beskyttelsen.

Det vurderes, at et borger ic-kort kan tilvejebringe den fornødne sikkerhed, så borgerne kan få adgang til egne personoplysninger i edb-registrene. Et ønske der i dag ikke findes en løsning på.

Borger ic-kortet kan give mulighed for elektronisk samtykke til videregivelse af personlige oplysninger. En anvendelse, der ikke arbejdes på, men som vurderes som velbegrundet.

Endelig vurderes det som relevant at benytte et borger ic-kort til at styrke persondata-beskyttelsen ved, at borgeren kan kryptere visse følsomme oplysninger i sin sag f.eks. i kommunens socialforvaltning.

I anvendelses-eksemplet **personlig legitimation** analyseres en anvendelse til personlig legitimation, dvs. til at dokumentere hvem man er, og en anvendelse til fysisk adgangskontrol.

Et generelt udstedt borger ic-kort vil være et meget effektivt id-kort. Det særlige ved anvendelsen identitetskort er, at den ikke lægges ind som en særlig kort-funktion, men findes i og med borger ic-kortets kortindehaver-identifikation og fysiske udformning. En funktionel vurdering er således, at et borger ic-kort er et identitetskort. Hvordan kortet anvendes til id-kort, er reelt udelukkende et regulerings-spørgsmål.

Det vurderes videre, at det er acceptabelt, at et borger ic-kort anvendes til fysisk adgangskontrol, men det forudsætter en lovregulering som nøje præciserer omfanget heraf.

I anvendelses-eksemplet **databærer af personlige oplysninger** analyseres en række anvendelser, hvor borger ic-kortet opbevarer forskellige personlige data.

Formålet med at anvende borger ic-kortet til databærer af personlige oplysninger kan bl.a. begrundes i et ønske om, at dataene er

til stede, når der er behov for dem, i og med at personen har dem på sig og kan tage dem frem. En anden begrundelse kan være et ønske om at undgå elektroniske spor ved at flytte data fra edb-registre til kortet. En tredje begrundelse kan være, at personen har en elektronisk databank med egne oplysninger og dermed kan give det bedste grundlag for f.eks. sags- eller lægebehandling.

Det fremgår af vurderinger af anvendelses-eksemplerne, at myndigheder mv. ikke kan se muligheder for at flytte data fra edb-registre til kort [56]. Fra analysen omkring sikkerheden ved kortet kan det konstateres, at større datamængder rejser backup-problemer, som der ikke findes en praktisk løsning på. Endvidere må der peges på den risiko, der opstår, hvis man samler store mængder følsomme personoplysninger på kortet. Oplysningerne kan gøres tilgængelige for uvedkommende og dermed medføre et indgreb i den personlige integritet.

I anvendelses-eksemplerne er der peget på muligheder for at benytte borger ic-kortet til mindre mængder aktuelle data. Det er vurderet, at backup-problemet bedre kan klares i disse tilfælde, dels fordi personen har en konkret interesse i korrekte data, dels fordi de i givet fald kan lægges ind på kortet igen.

I overvejelser om projektets praktiske udformning konkluderes det, at borger ic-kortet bør udformes med et fast antal kendte kort-funktioner. Det betyder, at man må forkaste ideen om at borger ic-kortet som databærer kan anvendes til en vifte af muligheder, som den enkelte kunne udnytte efter behov.

Disse overvejelser rejser spørgsmålet om ic-kort teknologien i det hele taget er den rigtige teknologi til at opnå de nævnte databærer-mål?

Man kunne f.eks. overveje om en almindelig 3,5" diskette ville kunne anvendes. Den kan opbevare betydelige datamængder - og er en enkelt ikke nok, kan dataene fordeles på flere. Et argument for ic-kortet er størrelsen, men diskettens beskedne størrelse gør, at det ikke giver vanskeligheder at bære den. Et andet argument er den beskyttelse af dataene ic-kortet giver. Man kan her først spørge, om det høje sikkerhedsniveau egentlig er nødvendigt, eller om det at personen opbevarer den ikke er tilstrækkeligt. Desuden kan data på disketten beskyttes på forskelligt niveau fra almindelig læse-beskyttelse af filen til kryptering. Endvidere kan data på disketten være dokumenter, der er underskrevet med en digital signatur og derfor har en høj integritet. Endelig kan nævnes, at udbredelsen af diskette-stationer er lige så udbredt som pc'ere mv., og derfor er det meget enklere at læse disketten. Disketten er desuden langt billigere end et ic-kort. I fremtiden vil vi måske altid have vores personlige assistent, en lille håndcomputer, på os. Den kan behandle data på en diskette (eller et andet medie) og kommunikere trådløst med vor hjemme-pc og her hente sikkert opbevarede data.

Det må således vurderes, at anvendelsen databærer af personlige oplysninger ikke er relevant for et borger ic-kort. Hermed er ikke sagt, at anvendelsen ikke er relevant, men den skal i givet fald opnås på anden vis.

I afsnit 4.A c blev anvendelsen stamdata beskrevet. Her har vi nok undtagelsen fra reglen ovenfor. Det må vurderes som hensigtsmæssigt, at disse data findes på borger ic-kortet og kan overføres elektronisk i forbindelse med kommunikation eller sagsbehandling.

I anvendelses-eksemplet **brugerbetaling** benyttes borger ic-kortet i forbindelse med betaling for en offentlig ydelse/service.

Det er vurderingen i anvendelses-eksemplerne, at borger ic-kortet ikke bør anvendes til penge eller som ihændehaverkort (dvs. der ikke er anden bruger-identifikation, end at man har kortet i hånden). Det skal tilføjes, at man ikke bør flytte sikkerhedsniveauet til en egentlig brugeridentifikation alene for at kunne benytte borger ic-kortet! Der kan derfor kun være tale om periodekort (måneds-, års-, frikort o.l.).

Anvendelse som kreditkort kan ske ved at anvende kortets øvrige funktioner til brugeridentifikation (pin-kode bærer). En sådan brugerbetaling er normalt i strid med et ønske om at undgå elektroniske spor, men accepteres i en række betalingsformer.

Det er vurderet, at et borger ic-kort kan anvendes til administration af brugerbetalings-ordninger.

Det er relevant at benytte ic-kort-teknologien til brugerbetalingskort, hvor man har eller ønsker at indføre en brugerbetaling.

Begrundelsen for at samle brugerbetalingsanvendelser på et borger ic-kort er et ønske om, at borgerne kun skal have et eller få kort. Da en række brugerbetalingskort ikke kan kombineres med borger ic-kortet, og da man, som omtalt ovenfor under systemudformning, ikke løbende kan oprette og ændre anvendelser, må det vurderes som mest hensigtsmæssigt, at brugerbetalingsanvendelser findes på særskilte kort.

c) Hvilke borger ic-kort?

Der er, som omtalt i overvejelser om dokument-mappe konceptet, ikke grundlag for at samle alle anvendelser på ét borger ic-kort.

I vurderingen af anvendelser som brugerbetalingskort konkluderes, at sådanne anvendelser findes på et eller flere særskilte borger ic-kort. Etablering af brugerbetalingskort vil være nøje knyttet til iværksættelse og administration af bestemte brugerbetalinger. Denne type borger ic-kort skal derfor ikke behandles nærmere her.

På baggrund af sammenfatningen har vi en række anvendelser, som handler om elektronisk identifikation og dokument-sikkerhed (underskrift, hemmeligholdelse). Et kort med sådanne funktioner kan kaldes for et *kommunikationskort*.

Fremfor at se målet om ét kort som et overordnet mål for borger ic-kortet, kan det ses som et mere begrænset forbrugerkrav i forhold til identiske anvendelser. Det ene udgangspunkt var de mange kort til bruger-identifikation (betalingskort og pin-koder). Her kan et borger ic-kort give mulighed for at samle forskellige bruger-identifikationer fra såvel den private som den offentlige sektor på et kort. Anvendelserne under register-kontrol er dels ligeledes en elektronisk bruger-identifikation (egenadgang og samtykke) og dels bærer af krypteringsnøgle. Anvendelserne digital underskrift og hemmeligholdelse er begge anvendelse af krypterings-teknikker og bærer af krypterings-nøgler. Disse anvendelser er sammenhængende og udgør et værktøj af sikkerhedsmæssig art for kort-indehaveren til elektronisk kommunikation og anvendelse af elektronisk informationsteknologi.

Anvendelsen til personlig legitimation såvel manuelt som maskinelt kan etableres som et *identitetskort*, der således er et tredje borger ic-kort. Det vil være naturligt, at anvendelsen stamdata er en del af et identitetskort.

Kommunikationskortet vil ved anvendelse af kortindehaver-identifikationen kunne anvendes til maskinel personlig legitimation. Den fysiske udformning af kortet med foto mv. af sikkerhedsmæssige årsager betyder, at kortet også vil kunne anvendes til manuel personlig legitimation. Identitetskortet er derfor en uundgåelig funktion ved kommunikationskortet.

d) Privatkort

På baggrund af den funktionelle vurdering kan der således foreslås et borger ic-kort med følgende kort-funktioner (som er nærmere beskrevet i afsnit 6):

Brugeridentifikation

- brugeridentifikation ved forskellig elektronisk kommunikation til edb-systemer, hvor brugeren er kendt, f.eks. nøgle til kommunalt egenservice-system; opbevaring af pin-koder og anden information, så borger ic-kortet kan erstatte betalings-kort og disses pin-koder,
- adgangskontrol til edb-systemer, så kortet erstatter/supplerer password,

Digital underskrift

- krypterings-nøglepar, der gør det muligt at afgive en uafviselig digital underskrift,

Brevhemmelighed

- kryptering af data, så breve og andre dokumenter ikke kan læses af uvedkommende,

Registerkontrol

- hemmeligholde (kryptere) personlige data i edb-registre,
- samtykke til videregivelse fra edb-registre,
- identifikation der giver adgang til egne data i edb-registre,

Personlig legitimation

- manuel og automatisk personlig legitimation,
- fysisk adgangskontrol,

Databærer: stamdata

- navn, adresse og personnummer på kortindehaver og evt. mindreårige børn.

Dette kommunikations- og id-kort vil blive omtalt som et *privatkort*.

Det er for alle disse kortfunktioner vurderet, at de kan implementeres på et ic-kort. Og det kan konstateres, at man ved at bruge ic-kortteknologien til disse anvendelser opnår en unik generel løsning, der ikke har noget teknisk alternativ. De enkelte

anvendelser vil kunne etableres i forskellige specifikke tekniske løsninger, der dog må vurderes som dårligere. Dels vil løsningen for den enkelte anvendelse være dårligere og dels vil man have en række løsninger for samme anvendelse og løsninger, der ikke hænger sammen.

Mål

Et generelt udleveret privatkort er en opbygning af en del af infrastrukturen for en åben datakommunikation, som vil præge hverdagen i fremtiden. Det anses som en samfundsopgave at sikre, at der kan foregå en åben datakommunikation, gennem standardisering, udbygning af datanet, uddannelse og information om datakommunikation. Kortet vil bidrage til en infrastruktur for den elektroniske kommunikation. For det første ved at skabe sikkerhed for borgerne ved at sikre korrekt identifikation mv. og beskyttelse af den personlige integritet og privatlivets fred. For de systemansvarlige ved at der kan udvikles mere sikre anvendelser og for samfundet ved at sikkerhedsniveauet generelt hæves. For det andet ved at gøre den elektroniske kommunikation (mere) tilgængelig for den almindelige borger og dermed skabe grundlag for besparelser i den offentlige sektor og nye produkter for erhvervslivet.

Privatkortet er endvidere en realisering af målet om ét kort i den mere begrænsede udformning, som blev omtalt i afsnit a) ovenfor. Kortet giver mulighed for at en række forskellige kort, der alle etablerer en bruger-identifikation, kan samles på et privatkort. Endvidere giver privatkortet en generel løsning på en række funktioner, som vi ellers vil få forskellige specifikke løsninger på.

De mere konkrete mål, der er identificeret for anvendelses-eksemplerne i afsnit 6, er:

Bruger-identifikation

* Pin-koder og betalingskort kan erstattes af borger ic-kortet
* Kortindehaveren kan dokumentere anvendelse af "betalingskortet"
* Mulighed for fælles konto og pin-kode inden for familien
* Borgerne skal have mulighed for en sikker identifikation ved selvbetjening og adgang til egne personoplysninger i kommunens edb-registre
* Den kommunale forvaltning får mulighed for at etablere egenservice på områder, hvor det ellers ikke er muligt
* Den enkelte får mulighed for en mere sikker adgangskontrol til personlige edb-systemer
* Mere sikre pc-baserede systemer og dermed et mere robust samfund.

Digital signatur

* Den enkelte har mulighed for at afgive en bindende elektronisk underskrift.

Brevhemmelighed

* Den enkelte får mulighed for at sikre at breve, dokumenter o.l. ikke kan læses af uvedkommende.

Registerkontrol

Hemmeligholdelse:

* Borgeren sikres fuld hemmelighed af visse typer oplysninger i en sag
* Sagsbehandleren sikres fortrolighed i sagsbehandlingen
* Tillidsforholdet mellem klient og sagsbehandler afspejles i data-behandlingen.

Samtykke til videregivelse:

* Mulighed for at udbygge sagsbehandlingsområder i kvikskranker
* Borgernes data i forskellige registre kan genbruges, uden at det krænker den personlige integritet.

Egen adgang:

* Borgerne får adgang til oplysninger om sig selv i de offentlige registre
* Borgernes kontrol med egne personoplysninger styrkes.

Personlig legitimation

* Etablere en sikker og generel personlig legitimation, som kan anvendes i alle situationer, hvor der er et legitimt behov
* Etablere en sikker fysisk adgangskontrol til steder hvor en sådan kræves.

Databærer: stamdata

* Mulighed for maskinel overførsel af stamdata
* Mulighed for at opbevare stamdata på egne børn.

I de følgende afsnit fremlægges en række forskellige overvejelser og forslag, som uddyber forslaget om et privatkort.

Kortudsteder

Der må tages stilling til hvem, der skal være kort-udsteder for privatkortet. Umiddelbart er der tre muligheder: en offentlig myndighed, f.eks. Indenrigsministeriet, en privat virksomhed og en mellemting, f.eks. en privat virksomhed på grundlag af en lovgivning.

Uanset den juridiske organisering vil kortudsteder bl.a. være ansvarlig for at

- udvikle specifikation for en ensartet brugergrænseflade i kort-systemet,
- udvikle specifikation for grænseflade til service-udbydernes virksomhed,
- godkende og implementere bruger-identifikation (pin-koder) fra service-udbydere,
- udlevering af kort og erstatningskort,
- udvikle og vedligeholde sikkerhedssystem, herunder kortindehaver-identifikation,
- udvikle specifikationer for kort og udstyr i kort-systemet og autorisere leverandører.

Desuden synes det nærliggende, at kortudsteder også fungerer som det nøgle-center, der er behov for i forhold til anvendelsen digital signatur.

Sikkerhed

Privatkortet er et værktøj til at etablere sikkerhed. Der må derfor stilles meget høje krav til sikkerheden ved kortet og sikkerhedsforanstaltningerne i kort-systemet. Disse krav er behandlet i afsnit 5. Her skal blot nævnes nogle punkter:

Ic-kortet skal være en tamper-resistent enhed og data i kortet skal være krypteret.

Udlevering af kortet skal ske personligt og under meget troværdige forhold.

Der oprettes et register over alle personer der har fået et privat-kort, som bl.a. indeholder et entydigt nummer for det enkelte kort. Nummeret kan benyttes til spærring af mistede/stjålne kort. Registreringen kan f.eks. foretages i nøglecenterets register i sammenhæng med den private nøgle eller i CPR-registeret.

Kortudsteder skal opbevare et backup-kort, primært med kortindehaverens private nøgle til digital signatur.

Helt central for sikkerheden er kortindehaver-identifikationen. Det foreslås, at der anvendes to kortindehaver-identifikationer: en otte-cifret (selvvalgt) talkode og en biokode (f.eks. et fingermønster).

Brugbarhed

Et privatkort skal principielt kunne bruges af alle, der ønsker det. Det betyder, at der må stilles høje kvalitetskrav til brugbarheden, og at der gennemføres forsøg og tests af, om kravene er nået.

Det må sikres, at kort-indehaverne møder en ensartet bruger-grænseflade, uanset hvor de anvender deres privatkort. Da privatkortet har en række anvendelser, må der lægges vægt på en velegnet dialog til kortindehaverens valg af anvendelse og data.

For komplekse anvendelser, som digital signatur og brevhemmelighed, som vanskeligt kan forstås i detaljer, må der lægges vægt på at sikre kortindehaveren overblik over anvendelsen og kontrol med de enkelte trin i anvendelsen.

Kortfunktioner - tjenester

Listen over privatkortets kortfunktioner ovenfor angiver de funktioner kortet kan benyttes til, men er ikke udtryk for de tjenester (programmel/data) og de dataelementer, der findes på kortet. En række anvendelser vil kunne benytte samme tjenester.

Udover kort-funktionerne findes der en række basisfunktioner på kortet:

- operativ-systemet, herunder kryptering af data i kortet,
- kortindehaver-identifikation,
- en logfil, som opbevarer data om kortets anvendelse

- brugerinterface med kommunikation fra kortet til læser/terminal.

I de følgende skemaer er vist program/data indhold og de anvendelser, der benytter disse.

Bruger-identifikation				
Tjeneste	S	Dataelementer	S	Funktion
Programmel/data til at vise dataelementnavn og hente data	I	bank, pin, kontonr. mv bank, pin, kontonr. mv benzinselskab pin, kontonr. mv . . . Kommune id, cpr-nr.	F F F F	Erstatte pin-koder Adgang til selvservice Egen adgang til edb-registre Samtykke til videregivelse
S: Status F: Fortrolig - I: Intern datafil				

Kryptering				
Tjeneste	S	Dataelementer	S	Funktion
Programmel/data til at danne nøgle-par efter RSA	I	offentlig nøgle privat nøgle	F I	Digital signatur Samtykke til videregivelse Brevhemmelighed Hemmeligholde data i en sag Adgangskontrol til edb-systemer Brevhemmelighed
Programmel/data til at danne en digital signatur	I			
Programmel/data til at kryptere med en off. nøgle og dekryptere med en privat nøgle	I			
Programmel/data til at danne DES nøgle ud fra tilfældigt tal	I			
Programmel/data til at kryptere/dekryptere tekst med DES	I			
S: Status F: Fortrolig - I: Intern datafil				

Stamdata				
Tjeneste	S	Dataelementer	S	Funktion

Programmel/data til at læse/ rette/skrive data	F	Navn Adresse Cpr-nummer	F F F	Overførsel af stamdata elektronisk
S: Status F: Fortrolig - I: Intern datafil				

Nogle kort-funktioner findes flere steder, fordi der findes alternative løsninger.

Det fremgår af disse oversigter, at der kun er syv tjenester i privatkortet. Det må således vurderes, at privatkortet teknisk kan udvikles. Tjenesterne i krypterings-skemaet er alle fastlagt i internationale standarder. Et kommunikations-kort med privatkortets anvendelser er ikke standardiseret, og heller ikke et arbejdsemne i de internationale standard organisationer. Svensk Standard foreslog i maj 1993 de nordiske standardiseringsorganisationer, at man igangsatte et sikkerhedsprojekt om et fælles nordisk identitetskort med anvendelse af et ic-kort [57] .

Fysisk udseende

Kortets format skal naturligvis følge de eksisterende internationale standarder. Med hensyn til placering af oplysninger, som kan aflæses på kortet bør der - så længe der ikke findes en standard for ic-identitetskort og ic-kommunikationskort - tages udgangspunkt i standarder for andre kort.

I figur 1 findes en skitse for personbevisets fysiske udseende. Udgangspunktet for dette fysiske udseende har været standarden DS2341: "Identitetskort. Opbygning og Informationsindhold". Der skal her blot gives en kort kommentar til de enkelte felter:

Forside:

Kortudsteder og logo: oplysning om hvad det er for et kort

Chip: kontakt-knappen til kortets chip

Underskriftsfelt: indehaverens underskrift (medtaget af hensyn til manuel identifikation og sikkerhed)

Blank: ubenyttet felt

Dato: udstedelsesdato (kan være relevant for visse anvendelser og have betydning ved fornyelse)

Kortindehaverens navn: fulde navn

Foto: foto (medtaget af hensyn til manuel identifikation og sikkerhed)

Bagside:

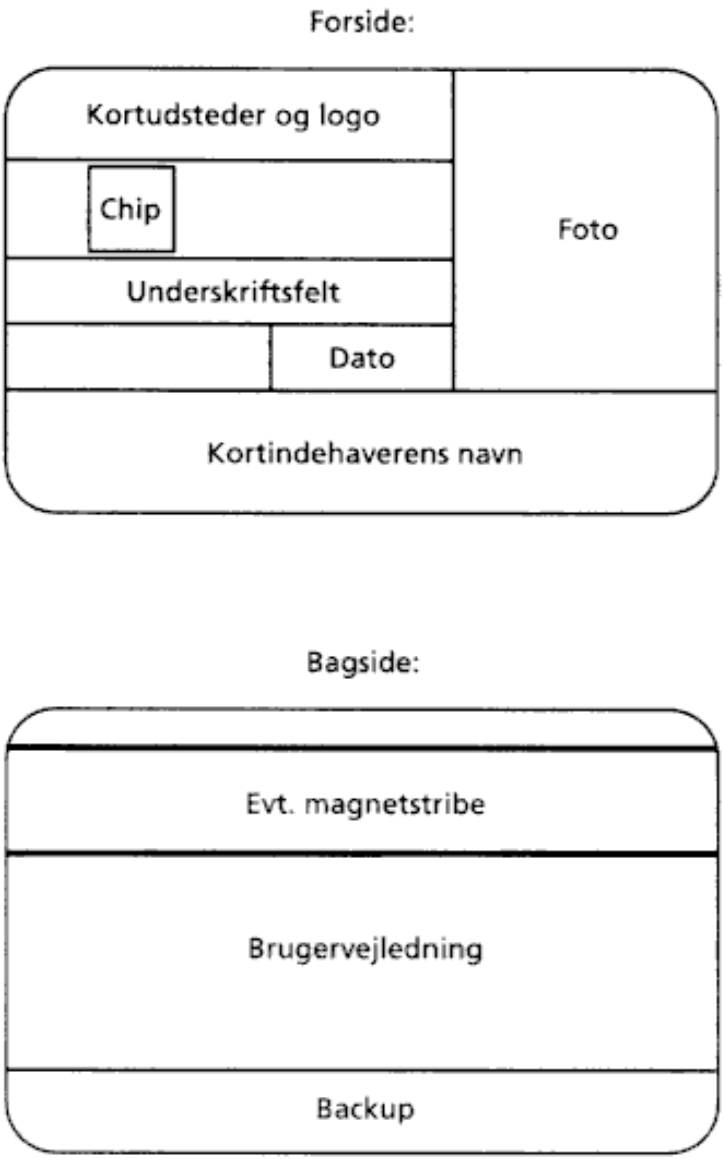
Magnetstribe: data på eksisterende kort (medtaget som en mulighed)

Brugervejledning: tekstfelt med oplysning om kortets anvendelse

Backup kort: tekstfelt, som oplyser hvor et backupkort opbevares.

Figur 1

Privatkortets fysiske udseende



7.B Økonomisk vurdering

Et element i vurderingen af et personbevis-system vil naturligvis være en økonomisk vurdering af systemets omkostninger og indtægter/besparelser. Den økonomiske vurdering kan kun være et element, fordi et evt. økonomisk slutresultat - positivt eller negativt - ikke i sig selv afgør om, privatkortet bør indføres.

En række forhold er vanskelige at kvantificere, f.eks. styrket retstilling og bedre service. Nogle eksempler:

- Aktiv og alsidig deltagelse i en elektronisk kommunikation.
- Styrket kontrol med og indsigt i personoplysninger i offentlige edb-registre.
- Lettelser ved at reducere antallet af kort hos den enkelte og specielt antallet af pin-koder.

Ved at sætte værdi på sådanne faktorer og derefter regne dem sammen med egentlige økonomiske forhold, får regnestykket

karakter af at "lægge æbler og pærer sammen". Det kan se pænt ud på papiret, men er dybest set noget vrøvl. Økonomien indgår i en helhed, der også omfatter funktionelle og etiske vurderinger. Disse vurderinger bør være grundlag for en beslutning.

Med økonomisk vurdering menes her alene en opgørelse af omkostninger og indtægter/besparelser. Denne økonomiske vurdering kan ske fra flere vinkler: kort-indehaveren, kort-udsteder, en service-udbyder og hele systemet (samfundet).

Kort-udsteder

Økonomien hos kortudsteder kan skitseres således.

Indtægter

- betaling fra kortindehaver?
- betaling fra serviceudbydere?
- reklameindtægter?
- tilknyttede funktioner?

Omkostninger

- etablering og drift af kortoperatør
- kort og backup-kort
- udlevering

Kortudsteder har mulighed for forskellige indtægter, men om de kan realiseres i praksis er et åbent spørgsmål.

Man kan tænke sig, at kortet helt eller delvist finansieres af en betaling fra kort-indehaveren. En sådan betaling er vel mest tænkelig, hvis privatkortet er et tilbud til borgerne?

Man kan videre tænke sig, at service-udbyderne betaler en afgift for de anvendelser de benytter. Det kunne f.eks. være fra private virksomheder (banker, firmaer med kontokunder) eller offentlige myndigheder (kommunerne, AF) som vil tilbyde, at man kan bruge privatkortet til PIN-kode-opbevarer eller anden bruger-identifikation.

Dernæst kan man tænke sig, at der tilbydes reklameplads på kortet. F.eks. kunne man tilbyde "reklamekort" gratis til kortindehaveren, mens almindelige kort havde en pris.

Endelig kan man tænke sig, at kortudsteder har nogle tilknyttede funktioner, der kan give indtægter. Det kunne f.eks. være at fungere som nøglecenter for krypteringsnøgler.

Kort-udsteders omkostninger er mere håndgribelige.

Omkostninger til kort-operatøren omfatter dels etablerings- og udviklingsomkostninger til udvikling af kortsystemet og herefter drift- og vedligeholdelsesomkostninger. Til illustration er Danmønt, som alene fungerer som system-operatør, etableret med en egenkapital på 80 mill. kr., som forventes anvendt til etablering, før Danmønt har fået en udbredelse, så der kommer indtægter.

Priser på kort er vanskelige at oplyse, da privatkortets udbredelse i sig selv må forventes at føre til prissænkninger. I dag oplyses prisen for et multifunktions ic-kort til ca. 100 kr. Back-up kortet må forventes at være en del billigere. Dvs. at udgiften alene til kort vil være o. 400 mill. kr.

Kortet skal udleveres ved kortindehavernes henvendelse til kortudsteder. Der er således en omkostning til organisering heraf og til særligt udstyr til initiering af kortet, indlæggelse af tal- og biokode, indlæggelse af bruger-identifikationer o.l. Engangsudgiften til udlevering af kort må forventes at skulle gentages efter 10 år.

Service-udbyderne

Økonomien hos service-udbyderne kan skitseres således.

Indtægter

- salg af service-ydelser
- besparelser

Omkostninger

- etablering og drift af anvendelser
- udstyr mv. hos brugerne

En udbygning af infrastrukturen til elektronisk kommunikation, herunder udlevering af et privatkort som generel sikkerhedsløsning, må antages at give nye muligheder for at udbyde informations-serviceydelser, f.eks. indkøb, fornøjelser og information.

Besparelser hos service-udbyderne ved de enkelte anvendelser kan i sagens natur kun vurderes konkret. Her skal nævnes nogle eksempler:

Overførsel af stamdata elektronisk f.eks. til oprettelse af en elektronisk sag, som kan antages at give en del besparelser. I en forundersøgelse til plast-sygesikringsbeviset henvises til, at udnyttelse af elektronisk overførsel af informationer fra magnetstriben vil give besparelser. Der sættes dog ikke tal på disse besparelser.

Mulighed for at udbygge egenservice. En lang række opgaver i det offentlige er egnet til egenservice, når der findes en sikker identifikation. Det antages, at der kan opnås betydelige besparelser.

Mulighed for at skabe elektronisk kommunikation fra borgerne til forvaltningen. Besparelserne ligger i forlængelse af de ønsker, der er om at udbygge anvendelsen af informations-teknologien i den offentlige forvaltning. Personbeviset giver mulighed for at borgerne indgår i denne udvikling og åbner dermed for ressource-besparelser [58].

Kontorchefen i KL's teknologikontor har skønnet, at en anvendelse, hvor borgerne ikke behøver at få tilsendt forskellige beviser, attester o.l. men i stedet selv kan hente dem i kommunens registre, når der er behov, vil kunne give milliardbesparelser [59]. Det må antages at private service-udbydere tilsvarende kan opnå besparelser. F.eks. er hele opbygningen af homebanking udtryk for, at der kan opnås besparelser.

I forbindelse med den enkelte anvendelse vil der være omkostninger til udvikling af edb-systemet og drift af dette.

Prisen på en kortlæser er afhængig af sikkerhedskravene til denne. Dernæst må man forvente et prisfald, hvis der indføres en generel anvendelse af et privatkort. I dag oplyses prisen til 1.000 - 2.000 kr.

Vurdering

Det har ikke været muligt inden for projektets rammer at foretage en egentlig økonomisk beregning. Det kan konstateres, at der er betydelige udgifter ved at få kort-systemet etableret. Udgifterne kan dækkes ind fra tre kilder: kort-indehaverne, service-udbyderne eller fra offentlige midler. Generelt kan man sige, at der er det økonomiske problem, at kort-udsteder har en række omkostninger, men ikke umiddelbart indtægter. Service-udbyderne har visse omkostninger, men det er hos dem, der er mulighed for indtægter, enten fra salg af ydelser eller i form af besparelser.

Betragtes privatkortet som en del af infrastrukturen og er kortudsteder finansieret over statsbudgettet er spørgsmålet, om man er villig til at betale omkostningerne for at skabe indtægter/besparelser hos offentlige myndigheder og private virksomheder.

Hvis kort-udsteder er et privat firma, bliver det afgørende, om der kan skabes indtægter hos kortudsteder.

Det er ikke muligt på dette grundlag, at sige om udlevering af et privatkort økonomisk er en "god forretning". Undersøgelser foretaget af konsulentfirmaet Fisher-Lorenz om etablering af datanet har vist, at man ikke kan forvente en økonomisk gevinst totalt set, men der kan opnås bedre effektivitet og service [60].

7.C Etiske vurderings-kriterier

På grundlag af funktionelle vurderinger er der i afsnit 7.A fremlagt et forslag om et privatkort. Man kan sige, at den funktionelle vurdering "kridter banen op" og fastlægger hvad der er muligt og derfor relevant at diskutere. De økonomiske betragtninger kan levere argumenter for og imod privatkortet ved at pege på udgifter, besparelser og fordele, som kan indgå i den endelige stillingtagen. Men er privatkortet en god ide? Dette spørgsmål kan hverken besvares ud fra funktionelle overvejelser eller ud fra økonomiske betragtninger. Her må tages stilling til privatkortets anvendelser og målene for dem. Er det godt eller dårligt for den enkelte at have et privatkort? Vil det fremme eller hindre en ønskværdig samfundsudvikling? Sådanne overvejelser om det gode liv med og for andre mennesker er etiske.

Der findes ikke en etisk videnskab eller metode, som kan føre os frem til saglige eller objektive konklusioner. Etikken har ikke en streng bevislogik, men er åben og bygger i princippet på den enkeltes holdninger. Dette afsnit kan derfor ikke ende op med en afsluttet vurdering af privatkortet. Der fremlægges en række etiske overvejelser struktureret som syv vurderings-kriterier.

Kriterierne er opstillet ud fra den generelle debat om anvendelse af elektronisk informations-teknologi i samfundet [61] og er de kriterier, der forekommer væsentlige for vurdering af privatkortet.

Grundlaget for overvejelserne er menneskerettighederne og dermed en tilslutning til de tanker, som Ole Thyssen fremlagde i bogen Teknokosmos [62] , nemlig at menneskerettighederne kan være grundlag for tekonologivurdering. Menneskerettighederne udgør et værdigrundlag der "på en gang er alment i sit indhold og juridisk i sin form - alment fordi det sætter den tekniske udvikling i forhold til samfundet som helhed og juridisk fordi det må bruges upersonligt" (s. 221) Menneskerettighederne er samtidig et fælles globalt sprog, som, uanset de kan synes svage og ikke respekteres, er en fælles platform, som ikke kan undsiges og har almen legitimitet. "De rummer et alment krav om, at samfundets teknik skal sikre det 'maksimalt minimale', som er den fælles frihed i samfundet" (s. 241). De er grundlæggende minimumsrettigheder og siger ikke, hvordan samfundet skal indrettes, eller hvordan edb skal anvendes. De stiller nogle rammer for en diskussion og stillingtagen, men giver ikke den praktiske løsning. De fortæller ikke hvordan vi skal leve, men opstiller betingelser for vores valgmuligheder. De indebærer en "moralsk ledetråd, et grundlag for vurdering af teknikken" (s. 243).

a) Deltagelse i elektronisk kommunikation

Privatkortet kan ses som en del af en infrastruktur for en åben datakommunikation (se afsnit 7.A d). I et fremtidigt samfund med en udbredt elektronisk kommunikation er det rimeligt at fokusere på en ret til at kommunikere, hvilket er en anden vinkel på forskellige grundlæggende rettigheder: ytringsfriheden, forsamlingsfriheden, privatlivets fred.

Men retten er ikke nok. Borgerne skal både kunne og faktisk anvende elektronisk kommunikation og serviceydelser. Bliver den i hovedsagen et anliggende for statsmagt og erhvervsliv, vil der opstå et skel i samfundet. Tænk f.eks. på et samfund, hvor telefonen ikke er almindelig tilgængelig.

Den etiske fordring er derfor, at et kommunikations-kort skal bidrage til, at den enkelte (flest muligt) er en aktiv og alsidig deltager i den elektroniske kommunikation.

Privatkortet kan på flere måde bidrage til aktiv og alsidig deltagelse:

Kommunikations-kortet er en sikkerhedsforanstaltning og kan bidrage til, at flere anvender elektronisk kommunikation ved at gøre anvendelsen troværdig og tryg. På den ene side vil den enkelte kunne anvende tilbud om elektronisk kommunikation, fordi det bliver generelt og umiddelbart muligt at benytte alle typer for elektronisk kommunikation sikkert. Og på den anden side kan der udbydes flere elektroniske serviceydelser, fordi der findes en løsning på det centrale problem, bruger-identifikationen.

Idag må vi acceptere de løsninger for bruger-identifikation, som service-udbyderne har indbygget. Med et privat kort i hånden kan den enkelte stille krav til de løsninger, der tilbydes. Man kan stille krav om, at den generelle og sikre løsning, som findes ved anvendelse af privatkortet, bruges. Den enkelte har i roller som forbruger, borger eller klient mulighed for at være en aktiv aktør i forhold til tilbud om anvendelse af elektroniske serviceydelser. Det kan f.eks. ske ved at sige nej tak til flere kort og pin-koder og i stedet kræve en løsning, hvor privatkortet anvendes.

Anvendelserne digital signatur og brevhemmelighed giver mulighed for at kunne kommunikere i åbne systemer. Med åbne systemer tænkes her på, at sender og modtager ikke behøver at kende hinanden før kommunikationen, i modsætning til lukkede systemer hvor senderen (f.eks. kunden) er registreret hos modtageren (firmaet, banken osv.) og har fået en særlig bruger-identifikation her. Privatkortet vil give den enkelte en styrket position ved valg af tilbud om elektronisk kommunikation.

Hvis privatkortet skal fremme deltagelse i den elektroniske kommunikation, er det afgørende, at kortet er let bruge og let at forstå. Dette blev behandlet i afsnit 8: brugbarhed.

b) Privat elektronisk kommunikation

I de kommunikationsformer vi traditionelt benytter, er der kendte spilleregler for troværdighed og hemmeligholdelse. Vi kan mødes og tale sammen uden, at det vedkommer andre, herunder statsmagten. Vi kan tale i telefon uden at andre lytter med. Der kan ved den personlige samtale og i telefonen indgås mundtlige aftaler. Aftaler kan indgås skriftligt og er troværdige, når de er underskrevet. Vi kan sende breve uden, at de åbnes (brevhemmelighed). Og vi kan indgå bindende aftaler ved at underskrive brevet (brevtroværdighed). Brevhemmeligheden er en direkte følge af den grundlæggende ret til privatlivets fred [63].

Når vi skal kommunikere elektronisk, er spillereglerne mere uklare, og borgerne har i almindelighed ikke et værktøj til at sikre brevhemmeligheden og brevtroværdigheden.

Det må anses for en ret også elektronisk at kunne kommunikere hemmeligt. Det er ikke tilfredsstillende, at der tilvejebringes specifikke løsninger i forbindelse med særlige serviceydelser, og det må derfor anses for en samfundsopgave at tilvejebringe en let tilgængelig mulighed for alle til at kommunikere privat.

Privatkortet opfylder denne etiske fordring med anvendelserne digital signatur og brevhemmelighed.

c) Robust samfund

Med robust samfund menes, at samfundet kan værge sig mod fjendtlige og kriminelle handlinger, politisk misbrug, ulykker, menneskelige svigt og andre hændelser, som får betydning for befolkningens velfærd og sikkerhed. Med udbredelsen af elektronisk informations-teknologi overalt i samfundet opstår en række sårbarheder. Hvis sikkerheden i de enkelte systemer er utilstrækkelig betyder det, at hele samfundet er sårbart. Det er således en samfundsopgave at medvirke til forbedring af sikkerheden for at opnå et mere robust samfund.

Til illustration kan man pege på, at det i trafik-politikken har været en særlig opgave at fremme trafiksikkerheden. Tilsvarende må det anses for en samfundsopgave at fremme edb-sikkerhed ved den elektroniske kommunikation. Samfundet har også en særlig sikkerheds-opgave, som består i beskyttelse af den personlige integritet og privatlivets fred.

F.eks. har den enkelte behov for at udføre en bruger-identifikation over for et edb-system i utallige sammenhænge. Svigter denne identifikation, åbnes mulighed for svindel og manglende tilgængelighed til systemerne. Denne identifikation er ikke forsvarlig, hvis den sker ved et - for den enkelte - uoverskueligt antal kort, koder og passwords. Det er et bidrag til et mere robust samfund, hvis bruger-identifikationen gøres mere sikker.

Privatkortet er en generel sikkerheds-foranstaltning, som vil kunne hæve sikkerhedsniveauet i samfundet og dermed give et mere robust samfund (i forhold til anvendelse af edb).

Omfattende sikkerhedsforanstaltninger og højt sikkerhedsniveau kan dog udvikle et risiko- samfund ved at skabe et mere truende risikobillede, end der faktisk findes. Omfattende sikkerhedsforanstaltninger kan måske endda i sig selv skabe risici og usikkerhed, f.eks. ved at hæve niveauet for kriminelle handlinger. Det er nødvendigt at spørge, om en teknologi, der kræver disse sikkerhedsforanstaltninger, fører til mere usikkerhed, end den giver fordele.

d) Persondata-beskyttelse

Persondata-beskyttelse er en grundlæggende rettighed, som det f.eks. er fastslået i Europarådets databeskyttelses-konvention [64], der skal beskytte den enkelte mod at personlige oplysninger indsamles eller anvendes så den personlige integritet undergraves.

Registerkontrol

I anvendelserne registerkontrol er vist nogle muligheder for at øge borgernes kontrol med egne personoplysninger i offentlige registre. Retten til at have adgang til egne oplysninger og retten til samtykke til videregivelse er to principper i databeskyttelsen. Der er beskrevet tre eksempler på anvendelser: egen adgang til de registrerede oplysninger, samtykke ved videregivelse og hemmeligholdelse af særligt følsomme oplysninger. Med disse anvendelser vil privatkortet styrke persondata-beskyttelsen.

Centrale registre

En række udenlandske eksempler på gennemførte eller planlagte id-kort viser, at der i praksis sker en sammenhæng mellem id-kort og centrale identitets-registre. Der er etableret centrale id-registre med forskellige personoplysninger og særlige identifikationer, herunder personnummer, størrelse, øjenfarve, digitaliseret underskrift og foto. I forhold til det danske cpr-register er der tale dels om et øget antal identifikations-oplysninger og dels om, at oplysninger, der findes i andre offentlige registre samles i id-registeret.

Registrering af persondata skal ske til nærmere bestemte og lovlige formål. Når der er tale om rent private oplysninger, må man endvidere overveje om registreringen af disse overskrider en "urørlighedszone", hvor den enkelte person har ret til at bevare oplysningerne for sig selv. Formålet med et omfattende centralt id-register vil bl.a. være at skabe bedre mulighed for at identificere den enkelte og for at det kan ske maskinelt. Videre må oplysninger som digitaliseret foto, underskrift o.l. betragtes som en overskridelse af, hvad der generelt bør registreres om befolkningen.

Det må således være et kriterium for indførelse af et privatkort, at der ikke samtidig sker en opbygning af et centralt

identitetsregister.

En anden sammenhæng mellem privatkort (som id-kort) og edb-registre findes, hvis det anvendes til identifikation til opslag i et edb-register. Denne procedure kan foretages i en personkontakt, f.eks. en samtale med en myndighedsperson, eller maskinelt, hvor kortet anbringes i en kortlæser, og opslaget i registeret sker automatisk. De registre, der primært har været tale om, er politiets kriminalregister og på europæisk plan Schengen-registeret over eftersøgte personer. En sådan anvendelse kan hverken helt accepteres eller helt afvises, men kan accepteres på bestemte betingelser. Det må være en forudsætning at proceduren gennemføres i en konkret sammenhæng, og i tilfælde som eksemplet med kriminalitetsregisteret, at der foreligger en begrundet mistanke. Omvendt må det afvises, at der etableres en generel automatiseret procedure.

Elektroniske spor

En følge af den stadigt voksende anvendelse af edb hos offentlige myndigheder og private virksomheder er, at der i stigende omfang opstår elektroniske spor om den enkeltes personlige forhold i forskellige databaser [65]. De registrerede data omfatter både følsomme oplysninger og almindelige, i sig selv ikke følsomme, oplysninger. Den risiko, der henvises til med elektroniske spor, er, at der med de mange data findes mulighed for at danne personprofiler og lignende. Det er en del af en databeskyttelse at tilstræbe en minimering af de elektroniske spor.

Ic-kort teknologien giver mulighed for at tilrettelægge edb-systemer, så der ikke dannes elektroniske spor. Privatkortet har ingen af denne type virkninger. Tværtimod kan man frygte, at privatkortets sikre brugeridentifikation kan føre til, at man i stedet vælger løsninger, som fører til elektroniske spor. F.eks. kan en brugerbetaling udformes med en kredit-konto i stedet for et forudbetalt kort, da man nu har privatkortet med brugeridentifikationen.

e) Individets kort

Ved udlevering af et privatkort, må der overordnet tages stilling til om kortet er kortindehaverens eller kortudsteders. Denne stillingtagen vil være afgørende for en række andre mål, specielt for anvendelse af privatkortet som id-kort.

Privatkortet er et værktøj til at anvende informations-teknologien (begå sig i informations-samfundet). Et værktøj for hvem? Svaret må entydigt være, at det er et værktøj for den enkelte kortindehaver. Betragtes kortet ikke som borgerens, påtvinges den enkelte et værktøj, som hun skal opbevare for andre og anvende, når det kræves. Det vil placere hende som et objekt i forhold til værktøjet og de edb-systemer, som det skal anvendes i samspil med. En sådan rolle må anses for at være i strid med den frihed, som er kernen i menneskerettighederne.

Kortet er ikke kortindehaveren

Når alle bliver udstyret med et privatkort, er der en risiko for, at man i forskellige sammenhænge lægger større vægt på kortets oplysninger, eller at kortet benyttes fremfor oplysninger fra den mundtlige kommunikation. Det er vigtigt, at være opmærksom på dette problem og fastholde, at kortet ikke er kortindehaveren, dvs. en distance mellem værktøjet, et ic-kort og personen.

Dette problem bliver sat på spidsen, når der opstår fejl ved kortet eller andre dele af systemet. Her vil kortindehaveren let komme i en pinlig situation og måske endog blive stemplet som snyder. Der er ikke umiddelbart nogen løsning, men holdningen, at kortet ikke er kortindehaveren, må afspejles i reguleringen, f.eks. om bevisbyrde ved tvivl.

f) Anvendelsen frivillig

Når først borgerne er udstyret med et privatkort, så vil - og selvfølgelig skal - dets muligheder anvendes, når offentlige myndigheder udvikler organisation og edb-systemer. De besparelser, der kan forventes, bør udnyttes. Men det må fastholdes, at det er frivilligt for borgeren, om han ønsker at benytte kortet og f.eks. deltage i en elektronisk kommunikation. Borgeren må kunne modtage den sagsbehandling eller service, han har krav på, uden at benytte kortet. Dvs. frivilligheden skal her forstås således, at borgeren skal have mulighed for ikke at anvende informations-teknologien til at kommunikere med det offentlige. Denne frivillighed er en fortsættelse af princippet om lighed for loven, som ikke bør begrænses af krav om at benytte en særlig teknologi.

En anden vinkel er, om det ligeledes skal være frivilligt at benytte kortet, når den enkelte ønsker at benytte elektroniske informations-serviceydelser? Hvis der f.eks. er tale om, at kortet skal benyttes til bruger-identifikation (nøgle) over for et egenservice-system, er anvendelsen af kortet et afgørende led i sikkerheden. Det må her være acceptabelt, at kortet kræves anvendt.

g) Frivillig personlig legitimation

Et generelt udstedt privatkort vil være et meget effektivt id-kort. Med id-kort henvises til en anvendelse af personbeviset til at gennemføre en personlig legitimation og dermed forbinde en persons fysiske identitet med den juridiske identitet. Umiddelbart kan det konstateres, at der i Danmark ikke er udstedt et identitetskort, som man har pligt til at bære på sig og forevise i bestemte situationer. Der er heller ikke forslag om at gøre det. Et identitetskort anses i almindelighed ikke for rimeligt eller nødvendigt.

Der er gode grunde til *ikke* at indføre et identitetskort af denne type. Et identitetskort må ses som et indgreb i den personlige integritet. Det giver grundlag for en øget overvågning og kontrol med befolkningen, f.eks. ved at kortet skal fremvises på forlangende eller bestemte steder (f.eks. lufthavne for at bekæmpe terrorisme); eller kortet skal anvendes ved bestemte handlinger (f.eks. banktransaktioner for at undgå skattesnyd). Der er tale om en generel mistænkeliggørelse af befolkningen. Denne øgede overvågning vil i første række blive oplevet af sociale grupper, som er specielle eller mistænkelige. Et id-kort med sådanne anvendelser vil stride imod kriterier, der er opstillet ovenfor:

- anvendelsen frivillig, idet identitetskort bygger på, at det kan kræves anvendt,
- kortet er ikke kortindehaveren, idet personen vil opleve, at man vil tage kortet som grundlag for hvem personen er.

Endelig skal peges på, at et generelt identitetskort vil være en hævelse af sikkerhedsforanstaltningerne i samfundet og dermed skabe et mere truende risikobillede.

Problemet er, at privatkortet ikke kan undgå også at være et identitetskort. Når en generel udnyttelse af denne anvendelse ikke ønskes eller helt afvises, kan man i stedet fremhæve, at privatkortet kun kan bruges til personlig legitimation i sammenhænge, hvor der er behov for det, og den enkelte selv ønsker at benytte kortet blandt andre alternativer. Det forudsættes således, at privatkortet kun benyttes, når den enkelte ønsker det. I en række sammenhænge har man behov for at kunne legitimere sig og benytter i dag forskellige dokumenter (pas, kørekort, dankort, sygesikringsbevis osv.). Denne legitimation opfattes ikke som overvågning, idet den har til formål at skabe sikkerhed ved en konkret sagsbehandling.

Hvordan privatkortet kan anvendes som et id-kort, er reelt udelukkende et regulerings-spørgsmål.

Man kunne mindske kortets anvendelighed som id-kort ved f.eks. at have et blankt kort uden person-oplysninger. En sådan udformning vil dog være i strid med sikkerhedskrav til privatkortet. Desuden vil kortet forsat kunne anvendes som id-kort til en maskinel legitimation, gennem kortindehaver-identifikationen.

Som kortudsteder kan man umiddelbart tænke sig en statslig myndighed, og her er det mest nærliggende Indenrigsministeriet. I forhold til privatkortet som infrastruktur og en bidragyder til en række samfundsopgaver vil det være en naturlig konsekvens, at det er en offentlig opgave at være kortudsteder. Men som følge af risikoen for et id-kort bør man overveje alternativer.

En anden mulighed er, at kortudsteder er et privat firma, som vil løfte denne samfundsmæssige opgave. Det skal ske på et lovgrundlag (Lov om kommunikations- og id-kort) og med et offentlig tilsyn. Tilsynet bør, af de samme grunde, som fører til at kortudsteder bør være en privat virksomhed, være en uafhængig myndighed, og der kan f.eks. peges på Registertilsynet. En sådan konstruktion vil muligvis bedre kunne sikre, at privatkortet kun blive anvendt til frivillig personlig legitimation.

Det er et afgørende etisk spørgsmål, om man tør løbe risikoen for, at et privatkort ændres til et id-kort, som kan kræves anvendt (manuelt og maskinelt) i en række situationer.

[55] SBA står for sårbarhedsanalyse og består af en række fremgangsmåder, teknikker og hjælpemidler til analyse af sårbarheden i edb-informationssystemer. SBA-projekt en metode til at identificere risici ved et projekt. Datacentralen (1987)
[56] Som konsekvens af konklusionen nedenfor om anvendelsen databærer af personlige oplysninger vurderes dette synspunkt ikke nærmere.
[57] Brev af 12/5-1993. Drøftet på et møde mellem en række nordiske standardiseringsorganisationer i Dansk Standard den 18. november 1993.
[58] Se afsnit 6.A b.
[59] KMD-Orientering september 1993.
[60] Oplyst af Thomas Skousen
[61] Ole Thyssen: TEKNOKOSMOS - om teknik og menneskerettigheder. (1985)
[62] John Bernhard, Thyge Lehmann: Den europæiske Menneskerettighedskonvention belyst gennem menneskerettighedskommissionens og -domstolens arbejde. (1985)
[63] John Bernhard, Thyge Lehmann: Den europæiske Menneskerettighedskonvention belyst gennem

menneskerettighedskommissionens og -domstolens arbejde. (1985)
[64] Europarådet Persondatakonvention: Om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (1981). Justitsministeriets bekendtgørelse nr. 59 fra 16. maj 1991.
[65] Ingvild Mestad: Elektroniske spor. Complex 3/86.

8. Høringssvar

En foreløbig version af nærværende rapport blev i februar 1994 sendt til høring hos en række interessenter. I dette afsnit optrykkes de afgivne høringssvar fra:

Indenrigsministeriet - CPR-kontoret,
Finansministeriet,
Kommunernes Landsforening,
Amtsrådsforeningen i Danmark,
Finansrådet,
Forbrugerrådet,
COII, Statstjenestemændenes Centralorganisation II,
Datacentralen.

INDENRIGSMINISTERIET

CPR-kontoret

Den 16. marts 1994

BEMÆRKNINGER TIL 'UDREDNING OM IC-KORT SOM BORGERKORT .

CPR-kontoret har med interesse studeret Teknologinævnets 'Udredning om ic-kort som borgerkort', som er fremsendt med Teknologinævnets brev af 23. februar 1993 med anmodning om bemærkninger.

Som supplement til rapportens afsnit 1.a 'Borgerkort på vej' kan

det oplyses, at Indenrigsministeriet i februar 1994 har iværksat

et forprojekt vedrørende ét elektronisk borgerkort. CPR-kontoret støttes i dette arbejde af en snæver referencegruppe med deltagelse af repræsentanter for Finansministeriet, Sundhedsministeriet, Amtsrådsforeningen og Kommunernes Landsforening, ligesom også andre berørte myndigheder og ekspertise på kortområdet vil blive inddraget i arbejdet. Til orientering vedlægges udkast af 4. februar 1994 til oplæg til dette forprojekt, som forventes afsluttet om ca. et halvt år.

CPR-kontorets bemærkninger skal derfor tages med det forbehold, at undersøgelserne i forbindelse med forprojektet kun lige er påbegyndt. Indenrigsministeriet har således ikke på nuværende tidspunkt lagt sig fast på en bestemt opfattelse af spørgsmålet om indførelse af et elektronisk borgerkort.

CPR-kontorets bemærkninger i det følgende er derfor ikke udtryk for en endelig vurdering af Teknologinævnets rapport, men alene bemærkninger af foreløbig karakter. En mere endelig vurdering vil bero på resultaterne at det forestående arbejde i forbindelse med for

projektet, hvori også inddrages Teknologinævnets vurderinger i den endelige rapport og debatten i forbindelse med rapportens behandling.

Forprojektet skal til sin tid danne det første grundlag for en stillingtagen til, om der - som led i videreudviklingen af CPRsystemet - skal søges opnået fornødent lovgrundlag til at indføre borgerkortet.

Baggrunden for Teknolpginævnets arbejde er en forventning om, at kortene vil komme, og at alle vil blive inddraget i elektronisk kommunikation med myndighederne og virksomhederne. Ud fra demokratiske, effektivitetsmæssige og samfundsmæssige betragtninger er det derfor efter Teknologinævnets opfattelse nødvendigt med en helhedsvurdering af denne teknologi, før borgerkortet udsendes.

CPR-kontorets undersøgelses udgangspunkt er for så vidt det samme, nemlig en forventning om, at der inden for det offentlige i de nærmeste år vil blive søgt etableret forskellige plastickortordninger, og derfor er et behov for en tidlig koordinering af disse bestræbelser i ét kort - det elektroniske borgerkort.

Forskellen er imidlertid, at Teknologinævnrapporten tager udgangspunkt i en bestemt produkt/teknik - nemlig ic-kortet (chip-, smart- og computer-kortet). CPR-kontorets undersøgelse tager derimod udgangspunkt i en analyse af behov og anvendelsesmuligheder og vil herefter lade dette danne grundlag for en vurdering af hvilken teknik, der i givet fald skal vælges.

Teknologinævns-rapporten indeholder imidlertid betragtninger omkring sikkerhed (afsnit 7), brugbarhed (afsnit 8) samt funktionel, økonomisk og etisk vurdering (afsnit 9), som - sammen med den debat og lægmandskonference, der er lagt op til, og den endelige rapport - vil kunne bidrage til belysning af væsentlige forhold i CPRkontorets forprojekt - uanset hvilken teknik og funktionalitet, der vil blive foreslået som resultat af forprojektet.

CPR-kontotets forprojekt vil - som det også er tilfældet med Teknologinævnets rapport - ikke kunne bekræfte eller afkræfte den indbyggede forventning i Teknologinævnsrapportens udgangspunkt om, at vi alle i løbet af få år (7 år ?) vil blive omfattet af elektronisk kommunikation som en helt naturlig del af hverdagen.

For så vidt angår rapportens konkrete forslag til et ic-kort som privatkort, som er fremkommet som resultatet af arbejdet, er CPRkontorets foreløbige vurdering følgende:

Anvendelsen af kortet som brugeridentifikation er relevant ved elektronisk kommunikation til edb-systemer, f.eks. som nøgle til kommunalt egenservice-system eksempelvis indtastning på en borgerterminal af oplysninger til skattevæsenets forskuds-/slutopgørelse, og som fremtidig adgangskontrol til edb-systemer primært for ansatte inden for det offentlige, men også i den private sektor, og ved adgangskontrollen til borgernes private PC'er. CPR-kontoret vurderer, at det navnlig er på dele af egenservice-området, hvor der stilles særlige krav til sikker identifikation af borgeren, at kortet vil kunne finde bred anvendelse, efterhånden som der opstilles borgerterminaler på rådhuset, biblioteket og banegården.

Derimod finder CPR-kontoret forslaget om, at benytte kortet til opbevaring af pinkoder og anden information, så kortet kan erstatte betalingskort og disses pinkoder, for unødvendigt. Problemet med de mange PIN-koder kunne allerede i dag løses, hvis de enkelte private kortsystemer, som der allerede ses enkelte eksempler på, lod borgeren selv vælge sin PIN-kode, der så kunne være fælles for såvel Dankortet, benzinkortet og til sin tid privat- eller borgerkortet. En sammenblanding af privat anvendelse til betalingsformidling og offentlig benyttelse af kortet er næppe hensigtsmæssig, bl.a... fordi det vil forøge risikoen for at kortet stjæles, hvis der er penge knyttet til det. En forenkling for borgerne på det 'private' kortområde ville derimod på sigt være en sammensmeltning af DAN-kortet og DANMØNT-kortet i ét kort til betalingstransaktioner.

Anvendelsen af kortet som digital underskrift og til sikring af brevhemmelighed lyder umiddelbart besnærende, men bygger på at vi alle privat anvender elektronisk post og anden elektronisk kommunikation. Godt nok har hvert 4. hjem i dag en PC og en del af disse kommunikationssudstyr, men spørgsmålet om digital underskrift og brevhemmelighed vil efter CPR-kontorets vurdering i de første mange år alene være et problem, der skal løses af hensyn til erhvervslivets og det offentliges udveksling af dokumenter. Det er her spørgsmålet om brevtroværdighed - integritet, autencitet og uafviselighed - og brevhemmelighed vil have betydning - og ikke den almindelige kommunikation mellem 2 mennesker - Alice og Bob.

Derimod kunne det være relevant at benytte kortet som led i registerkontrollen til at give borgeren adgang (egenaccess) til oplysninger om sig selv i offentlige registre. Dette kan dog kun have betydning, når borgeren selv møder frem og forlanger registerindsigt. Registerindsigten er en væsentlig garanti i persondatabeskyttelsen, men befolkningens interesse herfor er formentlig noget overvurderet. CPR-registret modtager således på årsbasis under 500 anmodninger om registerindsigt, som alle fremsendes skriftligt, dvs. uden at borgeren ville have mulighed for at præsentere sit borgerkort. Den elektroniske adgang til egne persondata i registre vil forudsætte nyudvikling af særlige applikationer til edb-systemerne, men vil ikke altid på tilfredsstillende vis kunne supplere de registrerede oplysninger og standardiserede feltbeskrivelser med den "menneskelige forklaring", som det er CPR-kontorets indtryk, at borgerne især efterspørger, når det drejer sig om, hvad der er registreret om de pågældende.

Borgerkortet kunne også finde anvendelse i visse situationer i forbindelse med borgerens samtykke til videregivelse af oplysninger om borgeren fra edb-registre. Det er ofte i øjeblikket sådan, at dette samtykke gives med borgerens underskrift på en blanket, som kan fremsendes fra borgeren til det offentlige. Det skulle dog nødigt med kortet blive sådan, at borgerne i større omfang end idag pålægges at møde frem hver gang en sag skal behandles hos det offentlige. Det er således først i takt med, at egenservice- systemer indføres, at borgerkortet i større omfang vil kunne benyttes til samtykke til videregivelse af oplysninger.

CPR-kontoret finder det imidlertid ikke nødvendigt som foreslået, at kortet skal bruges til at hemmeligholde (kryptere) egne data, idet den fornødne beskyttelse af specielt følsomme data i offentlige edb-registre normalt kan ske indenfor rammerne af den gældende registerlovgivning. For de i rapporten anførte eksempler på oplysninger om alkoholforbrug/misbrug, mulig skilsmisse,

børns tyveri, HIV positiv eller homoseksualitet gælder der efter § 9, stk. 2, i lov om offentlige myndigheders registre, at disse ikke må registreres, medmindre dette er nødvendigt for varetagelse af registrets opgaver. Det er således ikke oplysninger, som kan edbregistreres efter sagsbehandlerens forgodtbefindende, f.eks. i fritekstfelter i et offentligt edb-register. Er sådanne oplysninger relevante i en konkret sag, vil det efter CPR-kontorets opfattelse give større sikkerhed for den enkelte borger, at denne selv oplyste disse forhold eller at sagsbehandleren indhentede oplysningerne fra en anden forvaltningsmyndighed efter de derom gældende bestemmelser i forvaltningslovens S 28, stk. 2, end hvis oplysningerne i kortere eller længere perioder opbevares på kortet.

Kortet må helt klart finde anvendelse som personlig legitimation som kan benyttes i alle de situationer, hvor der er behov herfor. Omfanget heraf søges afdækket i CPR-kontorets undersøgelse af, hvorledes kortet kan overflødiggøre andre kort, attester og beviser, som der i dag er krav om, at borgeren skal fremvise over for det offentlige i forbindelse med sagsbehandling m.v. Med borgerkortet kan den enkelte identificeres sikkert, således at de nødvendige oplysninger i stedet kan hentes i de offentlige edbregistre uden at ulejlige borgerne. Kortets nærmere udformning, indhold og anvendelse skal fastlægges i lovgivningen. Det skal understreges, at der ikke i forbindelse med CPR-kontorets forprojekt er planer om at indføre krav om, at borgerne altid skal bære borgerkortet på sig og fremvise dette på forlangende.

Det vil endvidere være relevant at benytte kortet som fysisk adgangskontrol til f.eks. arbejdspladser inden for såvel offentlig som privat sektor, men der må formentlig fastsættes nærmere regler i lovgivningen, der regulerer dette forhold.

Efter gennemgang af en række eksempler på siderne 65 - 83 på kortet som databærer af personlige oplysninger munder rapporten ud i et forslag om, at privatkortet alene skal indeholde stamdata, som navn, adresse og personnummer og oplysninger om evt. mindreårige børn. Dette svarer ganske godt til CPR-kontorets foreløbige vurderinger af behovet, som dog også vil kræve et billede på kortet.

For så vidt angår personlige beviser udstedt af offentlige myndigheder, f.eks. kørekort, jagttegn fiskekort m.v. er det efter CPR-kontorets opfattelse ikke nødvendigt at opbevare oplysninger herom på selve borgerkortet, idet retten til f.eks. at køre bil allerede i dag fremgår af politiets registre, som politibetjenten kunne få adgang til ved anvendelse af borgerkortet, der entydigt identificerer og legitimerer personen, således at borgerkortet kunne erstatte kørekortet ved kørsel i Danmark. Tilsvarende vil også gælde for andre personlige beviser.

CPR-kontoret finder det ikke relevant at lægge op til et kortsystem, hvor der på selve kortet skal registreres oplysninger i forbindelse med generel/specialiseret helbredsjournal, vandrejournal i sundhedssektoren og recepter/midicinforbrug. Det er her CPRkontorets vurdering, at der i løbet af en kortere årrække vil være de nødvendige elektroniske kommunikationsmuligheder til rådighed, som vil løse problemerne med tilgængeligheden til disse oplysninger, f.eks. gennem etablering af et patientorienteret informations- og behandlingssystem, der gør patientens personlige og behandlingsmæssige data, herunder røntgen-billeder, laboratorieprøver m.v. tilgængelige uafhængig af sted.

Derimod kunne det efter CPR-kontorets opfattelse overvejes, om nød/advarselsoplysninger såsom f.eks. kroniske sygdomme, allergier, blodtype, vaccinationer samt evt. livstestamente og organdonor-

tilsagn til brug under akutte omstændigheder skal kunne opbevares på borgerkortet, hvis den enkelte ønsker dette. Men også her vil disse oplysninger i løbet af en kortere årrække kunne være tilgængelig uafhængig af sted gennem elektronisk kommunikation.

Spørgsmålet om tilfredstillende kortindehaver-identifikation fores*lås* i rapporten løst ved både anvendelse af en 8-cifret selvvalgt talkode (pinkode) og en såkaldt biokode, f.eks. underskrift, fingeraftryk, blodåre i håndfladen, stemmegenkendelse, blodårer i øjet, striber i iris, håndformen. omend man kan blive ganske fascineret af teknikkens muligheder på dette område, må det efter CPR-kontorets opfattelse vurderes nøje, om der er behov for en biokode i tilknytning til kortet. Dankortets 4-cifrede PIN-kode har gennem en årrække vist sig at være tilstrækkeligt, og der er jo her tale om adgang til betalingstransaktioner, hvor forbryderiske elementer nok skulle have udnyttet svaghederne, hvis det var muligt. Debatten og lægmandskonferencen vil være interessant i forbindelse med biokoder. Umiddelbart ledes tanken hen på Big Brother, hvis vi alle skulle aflevere f.eks. vort fingeraftryk til brug for kortets biokode.

En andet aspekt er økonomien. Det er tankevækkende, at Teknologinævnets forslag til 'privatkort' - det såkaldt multifunktions ickort - vil koste ca. 100 kr. pr. stk., dvs. mindst 400 mill. kr. alene for selve udstedelsen til alle på 16 år og derover. Noget kunne derfor tyde på, at en mere simpel løsning, som der er lagt op til i CPR-kontorets undersøgelse - alene af økonomiske grunde vil være mere realistisk end Teknologinævnets 'privatkort' .

Teknologinævnet anfører i et afsnit på side 105-106 om projektgennemførelsen ved multifunktionskortet, at "projektorganisationen kan blive karakteriseret ved, at der er mange systemejere fra såvel den offentlige som den private sektor. Endvidere kan beslutningerne i betydelig omfang blive politiske beslutningsprocesser. En sådan kombination er erfaringsmæssig

meget risikofyldt." Der ligger dog i Teknologinævnets forslag om privatkortet, at der skal tages en politisk beslutning om udstedelsen af kortet. Det er naturligvis

udgangspunktet for CPR-kontoret, at en eventuel indførelse af et borgerkort skal ske på grundlag af en politisk beslutningsproces, hvor kortets udformning og regler for benyttelse fastsættes udtrykkeligt i lovgivningen. Herudover skal der naturligvis i særlovgivningen være adgang til at fastsætte bestemmelser, hvorefter borgerkortet kan kræves forevist i forskellige situationer i stedet for f.eks. fisketegn, jagttegn, kørekort osv. og ved henvendelser til det offentlige.

Rapporten stiller spørgsmålet om kortudstederen skal være staten (Indenrigsministeriet) eller en privat organisation, hvor den sidstnævnte mulighed skulle sikre, at kortet kun bliver anvendt til frivillig legitimation. Der er ikke med CPR-kontorets borgerkortundersøgelse lagt op til et krav om, at den enkelte borger altid skal bære kortet på sig. CPR-kontoret finder det helt naturligt og nødvendigt - af hensyn til koordineringsopgaven, der skal forhindre fremkomsten af parallelle kortsystemer inden for det offentlige at staten, f.eks. Indenrigsministeriet, forestår udstedelse m.v. af et eventuelt fremtidigt borgerkort. Det er ikke sandsynliggjort, at et privat firma bedre kan sikre, at borgerkortet kun anvendes til frivillig personlig legitimation. Reglerne for anvendelsen er som nævnt et anliggende for Folketinget at fastsætte, mens administrationen bedst må kunne varetages i offentlig regie, hvor en minister i sidste instans er ansvarlig for overholdelse af lovgivningen.

Med venlig hilsen

TORBEN JERLACH

kontorchef

Finansministeriet

21. marts 1994

Foreløbig rapport fra Teknologinævnet - udredning om ic-kort

som borgerkort

Som det er Teknologinævnet bekendt, er der i Indenrigsministeriets regi igangsat et forprojekt om elektroniske borgerkort. I tilknytning til forprojektet er der nedsat en referencegruppe med deltagelse af bl.a. Finansministeriet.

Forprojektet skal navnlig ses på følgende baggrund:

De offentlige edb-registre rummer information, der gør det muligt at afskaffe meget af det papir, som den offentlige administration stadigvæk i høj grad er baseret på - forudsat at man foretager de nødvendige ændringer af administrative rutiner og forretningsgange. Et elektronisk identifikations- og servicekort til alle borgere er en mulighed, som bliver stadig mere interessant i takt med den teknologiske udvikling og den stigende udbredelse af elektroniske kort. Et elektronisk borgcrkort vil kunne fungere som "nøgle" til de offentlige edb-registre og må forventes at kunne erstatte/overflødiggøre en større eller mindre del af borgernes nuværende identifikationspapirer og -kort, f.eks. personbeviser, dåbs- og vielsesattester, sygesikringskort, kørekort, jagttegn etc. Det Centrale Person Register, CPR, vil være det naturlige udgangspunkt for et borgerkort.

Teknologinævnets udredning vil naturligvis indgå som et værdifuldt element i forprojektet. Forprojektet, som bl.a. skal belyse, om der er grundlag for at indføre et elektronisk borgerkort i Danmark, og hvilken teknologi der i givet fald skal anvendes, er imidlertid på et indledende stadium. På nuværende tidspunkt finder Finansministeriet det ikke muligt at tage endelig stilling til Teknologinævents vurderinger og forslag, mcn kan tilslutte sig de bemærkninger af foreløbig karaktcr, som er indeholdt i Indenrigsministeriets høringssvar af 16. marts 1994 til Teknologinævnet.

Med venlig hilsen

Olav Green-Pedersen

Kommunernes Landsforening

Den 17. marts 1994

Angående foreløbig rapport om IC-kort som borgerkort .

Teknologinævnet har i februar 1994 fremsendt en foreløbig rapport om IC-kort som borgerkort med anmodning om eventuelle synspunkter.

Indenrigsministeriet har den 16. februar 1994 iværksat et udredningsarbejde om elektroniske borgerkort, hvori resultaterne af Teknologinævnets arbejde vedr. IC-kort forventes at indgå.

l den anledning skal landsforeningen udtale, at man vil afvente Indenrigsministeriets udredning før stillingstagen til spørgsmålet om anvendelse af et elektronisk borgerkort.

Med venlig hilsen

Hans Sylvest

Amtsrådsforeningen i Danmark

Den 23. marts 1994

Høring om udredning om ic-kort som borgerkort

TeknologiNævnet har med skrivelse af 23. februar 1994 fremsendt en foreløbig rapport fra et udredningsarbejde om ickort som borgerkort med henblik på Amtsrådsforeningens bemærkninger.

Indledningsvist kan Amtsrådsforeningen tilslutte sig, at der er et behov for teknologivurderinger. I den sammenhæng må TeknologiNævnets initiativ hilses velkomment. Med de reelle muligheder, som redegørelsen peger på, for udviklingen af flere sideløbende kort, er det ligeledes fornuftigt, at man overvejer mulighederne for koordinering af denne udvikling.

Det bør i den sammenhæng nævnes, at Indenrigsministeriet har iværksat et forprojekt vedrørende et elektronisk borgerkort. Udgangspunktet for dette arbejde svarer meget til TeknologiNævnets. Der er imidlertid den væsentlige forskel, at Indenrigsministeriet ikke tager udgangspunkt i en bestemt teknisk løsning - som redegørelsens forslag til et ic-t - men tager udgangspunkt i en beskrivelse af de transaktioner, der involverer både borger og offentlige myndigheder, og som egner sig for en elektronisk kommunikation.

Amtsrådsforeningen deltager i den referencegruppe, der **skal** følge Indenrigsministeriets forprojekt. Det er aftalt i referencegruppen, at TeknologiNævnets redegørelse, som indeholder mange interessante aspekter, bør indgå i ministeriets og referencegruppens videre arbejde.

Amtsrådsforeningen vil derfor afgive sin vurdering af Teknologinævnets redegørelse i forbindelse med dette udvalgsarbejde.

Med venlig hilsen

Wayne Jensen

FINANSRÅDET

17. marts 1994

Ref.: Gert Bundgaard

Kommentarer til TeknologiNævnets foreløbige rapport om

IC-kort som borgerkort

Finansrådet finder det meget glædeligt, at TeknologiNævnet med rapporten om IC-kort som borgerkort starter en debat om denne nye kortteknologi. Pengeinstitutternes har utvivlsomt de mest oplagte anvendelsesområder for den nye teknologi. Pengeinstitutsektoren er derfor vigtig for chipkort-teknologiens udbredelse. Omvendt er chipkort-teknologien vigtig for pengeinstitutterne i fremtiden.

De danske pengeinstitutter ser meget gerne en offentlig debat om denne teknologi. Det er vigtigt, at der i offentligheden kommer en forståelse for, hvorledes chipkort virker og hvilke -muligheder der åbner sig med chipkort-teknologien.

Endnu vigtigere er det måske, at den offentlige debat kan fjerne mystikken om teknologien. Det er helt naturligt, at enhver ny teknologi giver anledning til betænkeligheder. Det er vigtigt, at der bliver en offentlig debat, hvor også urealistiske forestillinger om konsekvenserne af teknologien kan afkræftes.

Chipkort er dog en teknologi, som umiddelbart burde kunne modtages positivt af borgerne. Det er en teknologi, som i enhver betydning af ordet er tæt på borgeren. De data, der er lagret i et kort, vil borgeren selv få kontrol over. Dette vil være mere betryggende, end når de samme oplysninger registreres i centrale databaser.

Et eller flere kort?

TeknologiNævnets debatoplæg indeholder et eksempel på, hvorledes en række funktioner kan samles i et og samme kort. Eksemplet illustrerer på udmærket vis, hvilke muligheder kortet indeholder. Dog skal man passe på, at man ikke først og fremmest ser chipkort-teknologien som et redskab til at reducere antallet af plastikkort, som den enkelte borger skal håndtere.

Problemet med de mange forskellige kort bliver ofte overdrevet, og de problemer, der er, løses ikke alle ved at lægge flere funktioner på samme kort. Hvis chipkortet benyttes til at "opsamle" en række funktioner fra forskellige virksomheder og institutioner, vil der opstå et problem med at overskue hvilke funktioner, der er indlagt.

Betalingsfunktioner

Med hensyn til pengeinstitutydelser er det Finansrådets forventning, at de danske pengeinstitutter vil være betænkelige ved at indlægge funktioner fra pengeinstitutternes produkter på plastkort, der udstedes af andre end pengeinstitutterne selv. Betænkelighederne skyldes:

Sikkerhedsproblemer. Indlægning af f.eks. DankortPIN-koden i mikroprocessorens hukommelse kan muligvis udføres på en måde, som er sikkerhedsmæssig forsvarlig ud fra et teknisk synspunkt. Det vil imidlertid ikke være betryggende for pengeinstitutterne, hvis andre end pengeinstitutterne selv bliver ansvarlige for dette led i sikkerheden.

PIN-kodedisciplin. Et andet sikkerhedsmæssigt problem ligger i, at nogle af kortets funktioner vil have mindre sikkerhedsmæssig betydning end pengeinstitut-funktionerne. Der vil derfor være en risiko for, at kortets "fælles" PIN-kode afsløres i forbindelse med brug af de mindre sikkerhedskrævende funktioner.

Markedsføring. Pengeinstitutternes udstedelse af egne kort har en markedsføringsmæssig betydning for pengeinstitutterne. Det vil være vanskeligt for kunderne at huske og skelne mellem en lang række funktioner, som er indlagt på et og samme plastkort.

Afhængighed. I det omfang et offentligt udstedt multi-funktionskort får succes, vil både borgerne og serviceudbyderne komme til at stå i et afhængighedsforhold til den offentlige myndighed. For serviceudbyderne indebærer dette en risiko for politisk styring af, hvilke funktioner der kan ligge på kortet. Serviceudbyderne vil ligeledes blive afhængige af den kortudstedende myndigheds beslutninger om f.eks. introduktion af nye korttyper.

Ingen muligheder bør afskæres

Selv om pengeinstitutterne har mange betænkeligheder ved at integrere forskellige funktioner på samme kort, vil man være meget lydhør over for ønsker om samarbejde ved etablering af borgerkort.

Det førte skridt må være at skabe en offentlig debat, hvor bevidstheden om chip-kortenes virkemåde højnes. Herefter vil der kunne gennemføres egentlige undersøgelser af størrelsen af de behov, der findes i befolkningen og blandt institutioner og virksomheder for specifikke løsninger. Disse må så sammenholdes med de investeringer, der skal foretages, og de omkostninger,

der vil være ved driften af fælles systemer.

Endelig må det erindres, at chipkort-teknologien i de kommende år vil blive udbredt til en række formål - også selv om der ikke måtte ske en integration, hvor mange funktioner indlægges på et og samme kort.

FORBRUGERRÅDET

2. maj 1994

Kommentarer til Teknologinævnets foreløbige rapport - udredning

om IC-kort som borgerkort.

Forbrugerrådet ser med tilfredshed på TeknologiNævnets initiativ til en offentlig debat omkring de elektroniske chip-kort.-Det er vigtigt at starte debatten på et tidligt tidspunkt og inden kortene er taget i anvendelse i større omfang.

Forbrugerrådet finder det af afgørende betydning at en evt. indførelse af kortet vil respektere grundlæggende rettigheder så som den personlige integritet, fysisk sikring af persondata, adgang til egne data og lige adgang til kortet uanset sociale forhold eller funktionsnedsættelser. Desuden skal der konkret tages stilling til forbruger- og borgerkrav, så et evt. fremtidigt kort kan indrettes driftssikkert, privat og samfundsøkonomisk forsvarligt, brugervenligt, organisatorisk uafhængigt af særinteresser og under offentlig tilsyn. Under ingen omstændigheder kan det besluttes at indføre et privatkort uden en bred folkelig debat, samt omfattende information.

Forbrugerrådet finder, at sikkerheden er af helt central betydning med hensyn til kortsystemerne. Sikkerhedsmæssigt er

de nukendte kortsystemer (eksempelvis betalingskort) sårbare. Et af de grundlæggende problemer er, at kortholderen skal hemmeligholde pin-koden. Dette kan ofte være vanskeligt fordi pin-koden er svær at huske, specielt hvis kortet kun anvendes lejlighedsvis, ligesom der kommer flere og flere kort og et virvar af koder. En anden alvorlig sikkerhedsbrist i systemet er, at indtastningen af pin-koder i mange tilfælde let kan aflures. Det må derfor efter Forbrugerrådets opfattelse konstateres, at en biokode i mange tilfælde vil være at foretrække. Efter Forbrugerrådets opfattelse er det en fordel, hvis pinkoder og andre identifikationsmetoder i forbindelse med værdifulde eller følsomme oplysninger erstattes med eller suppleres med biokoder, eksempelvis fingeraftryk, hvis dette rent faktisk bliver økonomisk og sikkerhedsmæssigt forsvarligt. Det er som nævnt en udtrykkelig forudsætning at sikkerheden samtidig forøges, ligesom der bør være mulighed for alternative identifikationsmetoder, således at personer, som eksempelvis på grund af et handicap er ude af stand til at anvende identifikationsmetoden, minimeres.

IC-kortets meget sikre personlige identifikation åbner mulighed for, at borgeren kan få direkte adgang til oplysninger om sig selv i såvel offentlige som private registre. Dette har den klare fordel, at det kan understøtte borgerens adgang til og kontrol med anvendelse af oplysninger om egne forhold i registre samt give oversigt over hvilke oplysninger, der opbevares i disse. Mulighed for udvikling af selvservicesystemer på baggrund af et personligt identifikationskort, kan f.eks. medføre en betydelig lettelse for mange mennesker, og dermed et betydeligt forbedret serviceniveau. Denne mulighed må dog ikke medføre en indskrænkning i borgerens adgang til personlig kontakt og sagsbehandling eller reelle valg med hensyn til om kortet ønskes eller ej. Herudover finder Forbrugerrådet, at chip-kortet er velegnet til opbevaring af offentligt udstedte personbeviser etc.

Forbrugerrådet er også positiv med hensyn til brevhemmelighed og digital signatur m.v., selvom rådet ikke er i stand til at vurdere behovet herfor og muligheden for, at problemerne i denne forbindelse alternativt vil finde en løsning.

Forbrugerrådet er således generelt positiv overfor, at der indføres et offentligt elektronisk personbevis ved hjælp af et multifunktionskort, under forudsætning af at der tages en overordnet beslutning om, hvad det bør bruges til, og at der fastsættes nærmere regler for anvendelse og sikkerhed. I første omgang bør kortet alene anvendes til identifikation over for den offentlige sektor.

Efter Forbrugerrådets opfattelse er det af helt central betydning, at der ved indførelse af kortet tages hensyn til frivillighed og brugervenlighed, således at borgergrupper hverken tvinges ind i brug af eller afskæres fra anvendelsen af kortet og dets muligheder. Det er i den forbindelse af afgørende betydning, at en eventuel indførelse af et privatkort følges op af en omfattende information.

Med venlig hilsen

Søren Geckler Afdelingschef

STATSTJENESTEMÆNDENES

CENTRALORGANISATION II

17. marts 1994

Høring om "udredning om ic-kort som borgerkort"

Under henvisning til Nævnets brev af 23. februar 1994 skal vi hermed meddele, at CO II tidligere har kommenteret projektet, og herunder bl.a. henledt opmærksomheden på sikkerheden og mulighederne for misbrug af ic-kortet.

Efter gennemlæsning af rapporten finder CO II bl.a. anledning til at fremhæve følgende spørgsmål:

-Af hvem og hvorledes skal et evt. borgerkort administreres?

- Hvad er "prisen"?

Mange mennesker har kraftig modvilje mod at anvende "plastkort".

- Hvordan forholder man sig eksempelvis med børn, unge og pensionister?

- Hvad skal et evt. borgerkort indeholde af oplysninger og hvorledes sikres det, at oplysningerne ikke misbruges ved bl.a. registersammenkøringer - herunder følsomme oplysninger om sygdom, medicinforbrug mv.

-Hvem skal betale for kortet - brugerbetaling?

-Hvilken pris og regler skal gælde for udstedelse af

dubletkort ved beskadigelse, bortkomst o.lign.?

Udover de nævnte spørgsmål skal CO II desuden påpege sikkerheden omkring udstedelse, administration og brug af ic-kort som borgerkort, og ved gennemlæsning efterlades det indtryk om ikke rapporten i sine konklusioner "går for vidt" og måske vil have vanskeligt ved at vinde bred accept hos den almindelige borger.

Med venlig hilsen
Henning Frederiksen

DataCentralen

17. marts 1994

Kommentarer til teknologinævnets rapport

Datacentralen har med interesse gennemarbejdet Teknologinævnets 'Udredning om ic-kort som borgerkort'. Datacentralen kan besvare spørgsmålet på rapportens forside: 'Skal vi danskere have et privatkort?' med et ja.

Datacentralen siger ja, fordi vi mener, at mange behov kan imødekommes med et kort, og fordi nytteværdien for samfundet kan blive stor.

Teknologinævnets rapport er en teknologivurdering, hvor formålet er at vurdere mulighederne med en bestemt teknologi - chipkortet. Herrned tager Teknologinævnet udgangspunkt i hvilke muligheder, teknologien stiller til rådighed, og på denne baggrund vurderer Teknologinævnet, om mulighederne skal udnyttes. Datacentralen beskæftiger sig også med mulige anvendelser af ny teknologi, men vi tager primært udgangspunkt i at klarlægge, hvilke behov der findes. Bagefter vurderer vi hvilken teknologi, der bedst opfylder disse behov.

Adgang til oplysninger i offentlige og private registre.

Med udgangspunkt i identificerbare behov har Datacentralen vurderet, hvordan borgerne kan give tredje part adgang til personlige oplysninger, registreret i offentlige og/eller private registre. Hermed kan borgeren slippe for at medbringe diverse udskrifter og dokumenter til brug ved sagsbehandlingen, når relevante oplysninger kan hentes eller bekræftes direkte i de registre, hvor oplysningerne i forvejen findes.

Sagsbehandleren vil få overført korrekte oplysninger direkte til eget program. Data kan anvendes i sagsbehandlingen, og de kan behandles og lagres elektronisk. Sagsbehandleren sparer tid og slipper for at indtaste og kontrollere oplysningerne. Fejl- undgås, og programmerne kan få overført relevante data til den videre behandling.

Kort som nøgle til oplysningerne.

Løsningen er, som også Teknologinævnet påpeger, at borgeren selv giver tilladelse til, at data anvendes og overføres. Et elektronisk kort giver en høj grad af sikkerhed ved sådanne trans-

aktioner, og det er en enkel måde at give tilladelsen på, fremfor f.eks. at udfylde diverse formularer som dokumentation for at tilladelsen til overførslen er givet. Kortet giver mulighed for en her og nu løsning, og kortets stærke side er, at det giver borgeren mulighed for selv at deltage i processen.

Et sådant system med overførsel af data initierer af borgeren vil i mange tilfælde kræve ændret lovgivning. Det forudsætter, at dataejerne får de nødvendige muligheder for, at data kan anvendes anderledes, end tilfældet er i dag.

Den helt store anvendelse af kortet i forbindelse med oplysninger i centrale registre forventes dog først at vise sig ved udbredelse af selvbetjeningsterminaler.

Forenklet sagsbehandling.

Datacentralens overvejelser på dette punkt svarer til en vis grad til Teknologinævnets eksempler omkring samtykke til videregivelse i f.eks. en kvikskranke, men Datacentralen ser videre perspektiver, end Teknologinævnet lægger op til. Der er store muligheder for at forenkle sagsbehandlingen til fordel for såvel borgeren som offentlige og private institutioner.

Datacentralen mener, at det er en forudsætning for disse forenklede arbejdsgange initierer af et kort, at dette kort er alment udbredt og accepteret af såvel offentlige som private, altså et borgerkort eller et privatkort.

Eksempler på forenklet sagsbehandling.

Datacentralen har overvejet en del af de eksempler på adgang til data, som nævnes i Teknologivnævnets rapport i afsnit 6. Vi har også været inde på andre opgaver, hvor der er behov for en smidig adgang til oplysninger. Vi kan nævne følgende, hvor det skal understreges, at det kun er eksempler, hvor vi ikke har vurderet den konkrete sagsbehandling:

Eksempel: lån i bank.

Ved en lånesag i bank skal banken have en række oplysninger, som kortet kan bruges til at give adgang til:

lønoplysninger hos arbejdsgiver,

bankkonti og lån andre steder,

kreditforeningsoplysninger,

forsorsikringsoplysninger,

skatteoplysninger,

årsopgørelser,

kreditoplysninger,bilbogen.

Eksempel: lån i kreditforening.

Kreditforeningen kan have brug for oplysninger fra:

- lønoplysninger hos arbejdsgiver,

- banken,

- BBR-registeret,

tinglysning,
kreditoplysninger, årsopgørelser fra skatteväsenet.

Eksempel: klient på bistandskontoret.

Bistandskontoret kan være interesseret i dokumentation fra f.eks:

- A-kassen,
- kreditforeningen (terminen), - cpr (hjemmeboende børn), - skatteväsenet (egne og ægtefælles indkomstforhold), - banken - (formue forhold).

Et eksempel på hvordan alle ville have kunnet opnå en lettelse, hvis der på nuværende tidspunkt havde været et kort med mulighed for adgang til data, er den igangværende konverteringsbølge hos realkreditinstitutionerne. Hvis muligheden havde været der, kunne lovgivningen have været udformet, så konverteringerne kunne gennemføres, ved at borgeren kunne møde op i kreditforeningen og med sit kort hente næsten alle relevante oplysninger fra diverse registre.

Det er tænkeligt, at tilsvarende situationer opstår fremover.

De nævnte eksempler er muligheder. Nogle er mere realistiske end andre, og det er næppe relevant at iværksætte det hele på en gang.

Nødvendigt med lovgivning.

Datacentralen vil pege på følgende problemstilling, som bør indgå i overvejelserne om et privatkort, hvis kortet får den funktion, at det fungerer som nøgle til at borgeren kan få, og give andre adgang til oplysninger.

Når det bliver muligt at få nem adgang til at formidle informationer, kan sagsbehandlingen effektiviseres, og borgeren kan opnå en lettelse, men der er en risiko for, at borgeren sættes under pres for at give adgang til flere oplysninger end ønskeligt. Mulighederne for at udbygge et i starten uskyldigt udseende koncept er jo store.

Selv om systemet bygger på den filosofi, at borgeren selv skal give adgang til oplysningerne, via sit kort, kan der meget nemt opstå et pres på borgeren om at give adgang til oplysninger, som borgeren måske ikke er interesseret i, skal indgå i sagen. Ved at sige nej kaster borgeren jo en mistanke på sig selv, om at ville skjule noget.

Argumentet om, at det kun er de, der har noget at skjule, der kan have noget imod, at oplysningerne kommer frem, er besnærende, men det holder ikke. Problemet er, at når en mulighed **findes,** vil den også blive udnyttet, selv om det ikke er rimeligt i den pågældende sammenhæng. Borgeren kan dermed miste den reelle mulighed for selv at bestemme over anvendelsen af data.

Derfor er det nødvendigt, at lovgivningen beskæftiger sig med spørgsmålet. Det skal sikres, at borgerne får tillid til kortet, og at samfundets interesser tilgodeses.

Valg af kortteknologi.

Et kort med processor giver flest muligheder på længere sigt, men det er også muligt at sænke ambitionsniveauet og starte med en simpel chip, som kan klare identifikationsbehovet. Hvis konceptet tilrettelægges, så det er forberedt for en overgang til en processor chip, kan det udbygges fleksibelt i takt med at behovene opstår, og i takt med at det bliver økonomisk realistisk.

Kommentarer til udvalgte emner i Teknologinævnets rapport.

Datacentralen har konkrete kommentarer til problematikker omkring chipkortet, som ikke fremgår af Teknologinævnets rapport.

Standardisering.

Standardiseringsarbejdet er ikke endelig afsluttet endnu. Det kan tage flere år, før alle detaljer er faldet på plads. D. v. s at kortene eventuelt skal indføres samtidig med, at dette arbejde foregår. Det skal imidlertid ikke afholde nogen fra at gå igang, idet det grundlæggende standardiseringarbejde er afsluttet, så fundamentet for at gå videre med kortteknologien på en standardiseret måde er tilstede. Man skal blot tage højde for, at der løbende sker en udvikling inden for området.

Hemmeligholdelse af oplysninger hos en sagsbehandler.

Det er en unødvendig og omstændig sag, at opbevare krypterede oplysninger i det offentliges register. Udgangspunktet må være, at registerlovgivningen og forvaltningslovgivningen sikrer, at oplysninger registreret hos det offentlige, kun anvendes i den sammenhæng de er tiltænkt. Sagsbehandlingen skal foregå, så dette sikres.

Biokoder. Mulighederne er besnærende, men så vidt Datacentralen er orienteret, er der ikke udviklet løsninger, som anvendes i større stil.

Holdbarheden af kort.

En holdbarhed på ti år er den teoretiske holdbarhed for chippens elektroniske funktionsevne. Det er ikke efterprøver i praksis. Inden for denne mulige holdbarhed afgøres chippens levetid af kontakternes holdbarhed, og de udsættes for et stort slid i kortlæserne, hvorved holdbarheden reduceres.

Transaktionstider.

I forbindelse med valg af funktioner på et chipkort, er det nødvendigt at tage hensyn til transaktionstiderne. Kortteknologien er endnu på et niveau, hvor transaktionstideme kan være temmelig lange, og det kan sætte en grænse for hvilke funktioner, det er hensigtsmæssigt at indbygge i kortet.

Afslutningsvis vil Datacentralen rose det arbejde, der ligger til grund for Teknologinævnets rapport. Datacentralen tror, der er en fremtid for et chipkort, med en del af de funktioner rapporten lægger op til. Datacentralen mener, at en realisering af ideen om et processorkort til

danskeme, af økonomiske, teknologiske, etiske og politiske grunde ikke udføres på en gang, men vi ser Teknologinævnets arbejde som et vigtigt bidrag til en vurdering af mulighederne.

Med disse bemærkninger siger Datacentralen tak for en god, en saglig og en perspektivrig rapport. Vi ser frem til at følge resultatet af de drøftelser, rapporten lægger op til.

venlig hilsen

Jørgen Andersen

Afdelingsleder

9. Spørgepanelets slutdokument

I dette afsnit findes det slutdokument, som et spørgepanel af lægfolk udarbejdede på Teknologinævnets konference den 12. og 13. april. Panelets grundlag var en foreløbig udgave af nærværende rapport, en pjece som fremlagde forslaget om et privatkort, høringssvar fra en række interessenter (optrykt i afsnit 8) og oplæg fra en række eksperter. De spørgsmål som besvares i slutdokumentet var udarbejdet af Teknologinævnet.

Spørgepanelets sammensætning

Maria Barking, 54 år, lægesekretær, Frøstrup
Rose Jensen, 62 år, pensioneret sagsbehandler, Søborg
Maria Nørring, 42 år, psykoanalytiker, Charlottenlund
Olga Porotnikoff, 70 år, civilingeniør, Farum
Tina M. Pedersen, 26 år, cand. merc., Aalborg

Christian Hemdrup, 45 år, elektroniktekniker, Odense
Henrik Juul-Madsen, 20 år, samf. studerende, Aalborg
Ole Lund, 55 år, bankassistent, Hillerød
Aksel B. Michelsen, 37 år, Skørping
Arne Sv. Nielsen, 67 år, kontorchef, Herlev

Ekspertpanelets sammensætning

Gert Bundgaard, Finansrådet
Hasse Clausen, lektor, datalog, Datalogisk Inst., Københavns Universitet
Søren Geckler, Forbrugerrådet
Tom Jacobsgaard, Datacentralen
Torben Jerlach, kontorchef, Indenrigsministeriet
Oluf Jørgensen, lektor, cand.jur., AUC
Lars Klüver, projketleder, Teknologinævnets sekretariat
Peter Landrock, lektor, cand. scient., Ph.d.
Steffen Stripp, konsulent
Flemming Sørensen, journalist, Danmarks Journalisthøjskole

9.A Slutdokument

Informationsteknologien medfører en række sociale og kulturelle ændringer af vores liv og indbyrdes relationer. Og ikke bare ændringer i vores praktiske arbejdsgange. Indførelsen af et privatkort er kun et led i denne udvikling og er isoleret set måske ikke særlig betydningsfuld. Eksperternes udsagn og det fremlagte materiale fokuserer næsten udelukkende på tekniske aspekter, praktiske landvindinger og juridiske problemer, mens de kulturelle og samfundsmæssige aspekter forsømmes. Specielt savner vi vurderinger af informationsteknologiens indflydelse på aspekter som livskvalitet, arbejdsvilkår og borgernes oplevelse af overvågning.

Det er vigtigt, at der foretages en analyse af både borgernes og myndighedernes behov og en vurdering af de kulturelle og sociale konsekvenser ved en eventuel indførelse af kortet.

Vi vil understrege at brugen af et eventuelt kort skal være frivillig. Der må på ingen måde diskrimineres mod borgere, der vælger ikke at anskaffe et kort. Det bør sikres gennem lovgivning.

a) Spørgsmål 1: Hvilke funktioner skal privatkortet have?

a) Bruger-identifikation (pin-koder fra betalingskort, nøgle til selvservice-systemer osv.). Bør kortet sikre, at der kan laves en meget sikker identifikation af den person, der vil i kontakt med EDB-udstyr, som i forvejen "kender" personen? Det kan dreje sig om pengeautomater, ens egen PC, når den bruges til at komme i forbindelse med bankens eller kommunens EDB-systemer mm. Skal kortet kunne bruges som adgang til oplysninger i det offentlige og samtidig som f.eks. betalingskort. Bør kortet erstatte PIN-koderne på Dankort, VISA, Eurocard osv.?

Kortet bør kun bruges som adgangskort til oplysninger og serviceydelser i det offentlige og til private formål efter den enkelte borgers valg. Kortet må ikke bruges til kommercielle formål som for eksempel betalinger, kontokort, møntkort og privat adgangskontrol. Kommercielle virksomheder bør overveje at udvikle et fælles kort.

Der bør således være et klart skel mellem offentlige, private og kommercielle funktioner. Dels er bankerne og andre udstedere af

betalingskort øjensynligt ikke interesserede i at være med og kan næppe gennem lovgivning tvinges til at opgive de eksisterende kort som Dan-kort og Visa-kort. Dels har den mindst betydningsfulde funktion en tilbøjlighed til at præge den påpasselighed hvormed folk omgås kortet. Folk er tilbøjelige til at være mindre påpasselige med et kort, der bruges som lånerkort end med et kort, der bruges som betalingskort.

Borgerne skal have mulighed for at bruge kortet som elektronisk identifikation i forbindelse med kommunikation med andre borgere.

Kortet skal indrettes, så det med sikkerhed identificerer den person, der bruger kortet til kontakt med de offentlige myndigheder, registre og systemer. Sikkerheden i identifikationen skal tilpasses følsomheden af de oplysninger og ydelser, der ønskes adgang til. Sikkerheden ved brug af kortet som lånerkort behøver ikke at være så høj som sikkerheden ved søgning af følsomme oplysninger.

b) Digital signatur. Skal kortet laves, så det i forbindelse med bl.a. elektronisk post kan garanteres, hvem der sendte posten. Der kan med andre ord laves en slags EDB-underskrift, som ikke kan forfalskes.

Der skal være mulighed for at underskrive elektroniske breve og dokumenter på en sådan måde, at underskriften ikke kan forfalskes. For eksempel skal det være muligt at indsende og underskrive sin selvangivelse elektronisk. Men myndighederne må ikke tvinge borgerne til at indsende og underskrive dokumenter elektronisk.

Udvikling og indførelse af denne teknologi kan som sidegevinst give Danmark en teknologisk fordel, der kan gavne dansk eksport.

c) Brevhemmelighed. Skal kortet fungere så man sikrer, at kun den, man via sin PC'er sender et elektronisk brev til, kan læse det. Som det er nu, er elektronisk post meget nem at læse for andre.

Det skal være muligt at opretholde brevhemmeligheden, når man sender elektronisk post. Det skal ske i overensstemmelse med gældende lov gennem en funktion på kortet.

Det skal både være muligt at kryptere breve, der sendes via elektroniske postsystemer og breve, der sendes elektronisk direkte fra bruger til bruger. I det omfang udviklingen bevæger sig fra traditionel post til elektronisk skal det offentlige sikre et elektronisk kommunikationssystem mellem borgerne, der svarer til det nuværende postsystem.

d) Registerkontrol. Det kan sikres, at følsomme person-oplysninger i EDB-registre er ulæselige med mindre kortet og indehaveren er til stede. Kortet kan også indrettes så indehaveren skal give samtykke til samkøring eller videregivelse af registeroplysninger. Endelig kan det bruges til at give adgang til egne registeroplysninger, så man kan se, hvad der står i registrene og hvornår og af hvem, oplysningerne er blevet brugt. Bør kortet indrettes til disse funktioner?

Borgerne skal som minimum have adgang til egne registeroplysninger og mulighed for at følge myndighedernes anvendelse af disse data. Borgerne bør have adgang til disse oplysninger også uden et kort. Men kortet kan måske lette adgangen til de offentlige registre, fordi det er muligt at søge oplysningerne hjemmefra. Vi er opmærksomme på, at kortet kun giver borgerne adgang til rådata og ikke til myndighedernes tolkning af dem. Den demokratiske gevinst er derfor begrænset. Men vi mener dog, at borgernes adgang til egne data vil gøre myndighederne mere forsigtige og omhyggelige med lagring og anvendelse af oplysninger.

Mens borgerne skal have mulighed for at kontrollere myndighedernes brug af registeroplysninger, så skal myndighederne ikke have mulighed for at registrere, om en borger har skaffet sig adgang til oplysninger om sig selv.

Kortet skal indrettes, så indehaveren kan give samtykke til samkøring eller videregivelse af oplysninger. Myndighederne skal myndighederne have mulighed for at trække anonymiserede oplysninger til brug for statistik og videnskabelige formål uden samtykke.

Vi har sympati for tanken om, at følsomme personoplysninger skal sikres så godt som muligt. Men kortet skal gøre tilværelsen lettere for borgeren. Ikke mere besværlig. Derfor skal en eventuel yderligere sikring mod misbrug af følsomme oplysninger ske på en sådan måde, at borgeren ikke pålægges yderligere besvær.

e) Personlig legitimation. Skal kortet kunne bruges som legitimation over for f.eks. offentlige myndigheder, på posthuset eller måske ved adgang til arbejdspladsen. Der kan være tale om legitimation ved hjælp af billede og underskrift og ved hjælp af biokode, f.eks. fingeraftryk.

Kortet skal kunne bruges som legitimation på samme måde som et kørekort eller et sygesikringskort. Derfor skal der være billede

og underskrift på kortet. Men der må under ingen omstændigheder stilles krav om, at borgerne skal bære kortet som identitetskort med henblik på kontrol af politi og andre myndigheder. Kortet med dets elektroniske del skal kunne bruges som legitimationskort over for offentlige myndigheder.

Over for private må kun kortets visuelle del bruges. Private arbejdsgivere skal ikke kunne kræve, at medarbejderne anskaffer sig et borgerkort med henblik på elektronisk adgangskontrol.

f) Stamdata. Bør kortet rumme oplysninger om navn, adresse, personnummer for kortets indehaver og dennes eventuelle mindreårige børn?

Kortet skal rumme oplysninger om navn, adresse og personnummer. Om det også skal rumme oplysninger om mindreårige børn, skal afklares nærmere. Blandt andet skal det undersøges, om børn kan få deres eget kort.

g) Andre. Udredningen gennemgår en række andre funktioner, som det konkluderes, at kortet ikke bør rumme. Mener panelet, at de alligevel bør findes på kortet? Det kan f.eks. dreje sig om følgende funktioner: Sundhedsjournal, sagsoplysninger i forhold til a-kasse, bistandskontor, kørekort, jagttegn mm.

Oplysninger, der ligger i offentlige registre, som kortet giver borgeren adgang til, behøver ikke at ligge på kortet. Men det kan overvejes, om borgeren skal have mulighed for at indlæse oplysninger på sit kort og opbevare dem midlertidigt. Det vil eksempelvis gøre det muligt at indlæse og medbringe medicinske data til udlandet på sit kort.

b) Spørgsmål 2: Hvordan opnås en tilfredsstillende kortindehaver-identifikation?

a) Tal-kode (otte cifre, selvvalgt) som vi kender det fra Dankort, men med flere end de fire cifre.

b) Bio-kode (hvilke er acceptable, hvilken er den foretrukne). Bio-kode kan laves udfra f.eks. fingeraftryk, iris, digitalt billede, underskrift, stemme, håndflade mm.

c) Begge koder, som det foreslås i udredningen. Skal det i så fald være frivilligt at bruge bio-koden eller skal den kunne forlanges anvendt i bestemte situationer? Skal kortindehaveren kunne "sætte kortet" til kun at kunne bruge bio-kode?

Vi lægger stor vægt på sikkerhed, men også på brugervenlighed, også for handicappede og ældre. Hvordan det bedst opnås anser vi for et teknisk spørgsmål, som ligger uden for hvad et lægmandspanel kan vurdere.

c) Spørgsmål 3: Hvem skal udstede privatkortet, og hvordan kan det finansieres?

a) Bør kortet udstedes af staten, en privat virksomhed eller en privat virksomhed reguleret af en lovgivning? Hvad er fordele og ulemper ved disse forskellige løsninger?

Kortet skal udstedes af en offentlig myndighed, og dets anvendelse skal reguleres gennem lovgivning.

b) Der er flere mulige finansierings-løsninger. Det kan betales over skatten. Eller ved at den enkelte betaler for kortet. Eller ved at man betaler for at bruge det. Eller ved at service-udbyderne f.eks. banken betaler for at "komme med" på kortet. Hvad anser panelet for bedst?

Det drejer om så relativt små beløb, at finansieringsformen af selve kortet ikke er afgørende.

d) Spørgsmål 4: Hvad er den samlede vurdering?

Skal vi danskere have et privatkort? Hvorfor eller hvorfor ikke?

Vi kan ikke stoppe den teknologiske udvikling - databaser, regneark, tekstbehandling, EDB-kommunikation osv. er kommet for at blive og vil blive udviklet yderligere. Men har vi behov for at regulere denne udvikling - og hvis vi har, er et kort, som det skitserede, så en god løsning? Eller ligger der skjulte farer i kortet, som gør at det ikke er ønskværdigt overhovedet?

Vi ønsker ikke at stoppe teknologisk udvikling, men at regulere og styre den.

Borgerkortet synes, med de anvendelsesområder og begrænsninger, som vi har nævnt, ikke at have den store revolutionerende betydning, men vil formentlig heller ikke forpeste vores hverdag. Kortet berører ikke de væsentlige sider i vores liv og synes ikke at være af større betydning.

Blandt de mulige gevinster er en øget mulighed for demokratisk kontrol med myndighedernes brug af oplysninger gennem lettere adgang til aktindsigt. Desuden rummer kortet nogle praktiske anvendelsesmuligheder som for eksempel sikring af elektronisk post mellem borgere og mellem borgeren og myndighederne.

Blandt de mulige farer er en øget oplevelse af overvågning, et muligt skridt på vej mod teknokrati og fremmedgørelse og vanskeligheder ved at opretholde reel frivillighed i det lange løb.

10. Afslutning

Efter at have gennemført en udredning, en interessenthøring og en konsensus-konference, skal der i dette afsnit gives et bud på at få vurderingerne til at hænge sammen. Udredningen pegede på en række anvendelser af ic-kort-teknologien, som det kan være relevant at iværksætte. Den samlede pulje af sådanne anvendelser blev fremlagt som et fiktivt "privatkort". Interessenterne reagerede skriftligt på dette privatkort og nogle af dem fremlagde deres holdninger på konsensuskonferencen. Endelig skrev lægmands-panelet i løbet af konsensuskonferencen et slutdokument, hvori de redegør for deres holdninger til privatkortet og giver deres forslag til løsninger.

I dette kapitel er det hensigten at udøve den svære kunst at få disse, ofte divergerende, bidrag til at hænge sammen i et hele.

Kapitlet er opdelt i 4 afsnit:

a) Behovet for vurdering og debat
b) Kort-funktioner, der ikke er ønskede
c) To kort kan være løsningen
d) Forudsætninger for kortene

a) Behovet for vurdering og debat

Spørgepanelet peger i slutdokumentet (afsnit 9) på behov for bredere vurderinger af informationsteknologiens konsekvenser. Panelets vurdering er, at indførelse af ic-kort ikke i sig selv er særlig betydningsfuld eller vil have større samfundsmæssige eller sociale konsekvenser.

Udredningen bygger på den forventning, at elektronisk kommunikation vil blive en almindelig del af hverdagen (se afsnit 1 b). Den bredere vurdering må umiddelbart dreje sig om konsekvenserne af en sådan omfattende brug af elektronisk kommunikation i samfundet. Men det må konstateres, at man ikke kan forudsige meget om konsekvenserne for de aspekter (livskvalitet, arbejdsvilkår, og borgernes oplevelse af overvågning), som panelet efterlyser. Det er næppe muligt at forudsige og dermed vurdere konsekvenserne generelt, men der kunne f.eks. opstilles en række krav til det fremtidige elektroniske netværk, så det gav de bedste muligheder. De etiske vurderings-kriterier, der er opstillet i afsnit 7.C ligger i forlængelse af principper, der er opstillet i den amerikanske debat [66]. I udredningen peges der på de anvendelser, hvor ic-kort vil være en hensigtsmæssig løsning, taget disse principper i betragtning.

I høringssvaret fra Indenrigsministeriet, CPR-kontoret bemærker man, at ministeriets undersøgelse tager udgangspunkt i "en analyse af behov og anvendelsesmuligheder og (man) vil herefter lade dette danne grundlag for en vurdering af hvilken teknik, der i givet fald skal vælges." Amtsrådsforeningen skriver, at undersøgelsen tager udgangspunkt i en "beskrivelse af de transaktioner, der involverer både borgere og offentlige myndigheder, og som egner sig for en elektronisk kommunikation." Datacentralen skriver "..vi tager primært udgangspunkt i at klarlægge hvilke behov, der findes. Bagefter vurderer vi hvilken teknologi, der bedst opfylder disse behov."

I Teknologinævnets projekt har udgangspunktet været, at ic-kort fra forskellig side er fremlagt som en løsning på forskellige behov eller problemer. En væsentlig opgave har derfor været at analysere om ic-kort rent faktisk er en relevant løsning. Dernæst har udredningen påvist yderligere behov, hvor ic-kort kan indgå i en løsning.

Når man tager udgangspunkt i behov er det helt afgørende, hvis behov der undersøges. Man kan frygte, jfr. Amtrådsforeningens beskrivelse, at sigtet i Indenrigsministeriets undersøgelse gøres for snæver. Det er vigtigt at understrege, at man må inddrage behov, som borgerne har og behov der opstår med en udvikling af elektronisk kommunikation. Kommentaren i Indenrigsministeriets høringssvar, at brevtroværdighed og brevhemmelighed "alene må være et problem, der skal løses af hensyn

til erhvervslivets og det offentliges udveksling af dokumenter" må f.eks. afvises i en tid, hvor elektronisk kommunikation udvides på alle leder af samfundslivet.

Som det blev sagt på konferencen "der er ikke 5 mill. danskere, som står og råber på at få et borgerkort", eller med spørgepanelets ord "kortet berører ikke de væsentlige sider i vores liv og synes ikke at være af større betydning". Det synes at være vanskeligt for borgerne at tage stilling til fremtidige kort, som på nuværende tidspunkt kan synes mere eller mindre ligegyldige. På den anden side er det netop før kortene udstedes - eller alternative løsninger vælges - der skal tages stilling til mulighederne. Denne modsætning stiller krav om, at planer og politikker løbende lægges ud til offentlig debat.

b) Kort-funktioner, der ikke er ønskede

Det må ud fra udredningen, interessenthøringen og konsensuskonferencen vurderes, at følgende funktioner ikke er relevante i eventuelle fremtidige kortløsninger.

Identitetskort

Spørgepanelet understreger, at "der under ingen omstændigheder må stilles krav om, at borgerne skal bære et kort, som et egentligt identitetskort med henblik på kontrol af politi og andre myndigheder".

Der er så vidt vides ikke planer om et sådant identitetskort. Dette understreges også i Indenrigsministeriets høringssvar.

På den baggrund kan det fastslås, at der hverken er behov for eller ønske om at indføre et identitetskort. På grund af den risiko for udvikling af øget overvågning og kontrol med borgerne, som et identitetskort indebærer, må det derfor afvises, at borger ic-kortet bliver et egentligt identitetskort.

Databank for personlige oplysninger

I udredningen analyseres en række eksempler på anvendelser af et ic-kort til bærer af personlige oplysninger. I den funktionelle vurdering (afsnit 7.A b) konkluderes det, at denne anvendelse ikke er relevant for ic-kort, da denne teknologi næppe er den mest hensigtsmæssige. Der peges i udredningen på, at man idag f.eks. kan anvende en almindelig 3,5" diskette. Den umiddelbare fordel ved at bære oplysningerne på et ic-kort er at kortet fylder lidt og at det er meget sikkert. De afgørende ulemper er behovet for back-up og den begrænsede kapacitet i kortet. Disketter fylder nu meget lidt, er billige og de kan ved hjælp af kryptering gøres uhyre sikre. Dertil kommer, at borgerne oftest selv kan lave back-up af disketter.

Det kan anbefales, at der gennemføres mere detaljerede analyser af sådanne muligheder og udvikles konkrete løsnings-forslag. Behovet for at tage stilling til denne anvendelse skal ses i lyset af, at der i EU og den europæiske standardiserings organisation anvendes betydelige ressoucer på sundhedskort, som også skal bære personlige helbredsoplysninger.

Brugerbetaling

På baggrund af anvendelseseksemplerne (afsnit 4.G) vurderes, at ic-kort teknologien er relevant at benytte til brugerbetaling og et borger ic-kort kan anvendes til administration af brugerbetaling. Men i udredningens samlede funktionelle vurdering (afsnit 7.A) konkluderes, at sådanne anvendelser bør findes på særskilte kort. Brugerbetalings-kort vil være snævert knyttet til iværksættelse og udformningen af den enkelte brugerbetaling og en række bruger-betalingssytemer vil ikke kunne kombineres med et generelt borger ic-kort.

Såfremt en brugerbetalings-ordning alene anvender en elektronisk bruger-identifikation vil et borger ic-kort kunne anvendes. Men med baggrund i spørgepanelets bekymring for øget overvågning bør det tilstræbes, at brugerbetalingen tilrettelægges så den kan administreres uden der dannes elektroniske spor i centrale registre. Det vil i givet fald være vigtigt på grund af princippet om frivillighed, at etablere parallelle systemer, som kan fungere uden at borgerkortet er tilstede.

Penge

I udredningens afsnit 4.G a) er analyseret mulighed for at opbevare elektroniske "penge" på kortet til betaling af offentlige ydelser/service.

I udredningen påpeges at sammenblanding af penge-funktion og andre funktioner vil gøre kortet tyvetækkeligt, fordi der så ligger rede penge på kortet, og derfor vurderes det, at pengekort ikke skal have andre funktioner. Den løsning som firmaet DANMØNT er igang med opbygge, et landsdækkende åbent system med pengekort på op til 300 kr., må vurderes som helt tilfredsstillende.

Det kan således vurderes, at der ikke er behov for borger ic-kort med penge til f.eks. offentlige serviceydelser.

Personlige beviser

Det er i udredningen (afsnit 4.F b) blevet overvejet om et borgerkort skal erstatte forskellige personlige beviser, f.eks. sygesikringskort, cpr-bevis og kørekort. Det er vurderet, at det ikke er hensigtsmæssigt at indlægge beviser elektronisk i kortet. Men borgerkortet kan erstatte et bevis ved at give adgang til det offentlige edb-register, hvor de relevante oplysninger findes. Myndigheden kan på den måde få adgang til de oplysninger som ellers skulle aflæses på beviset.

Denne vurdering udbygges af spørgepanelet, der har som et bærende princip for et borger ic-kort, at det skal være frivilligt om og hvornår den enkelte vil benytte kortet (uddybes nedenfor). Denne frivillighed vil ikke kunne opretholdes, hvis borger ic-kortet skal anvendes som et personligt bevis, myndigheder kræver i bestemte situationer.

c) To kort kan være løsningen

Den helt centrale vurdering i spørgepanelets slutdokument er: "Kortet bør kun bruges som adgangskort til oplysninger og serviceydelser i det offentlige og til private formål ... Kortet må ikke bruges til kommercielle formål som for eksempel betalinger, kontokort, møntkort og privat adgangskontrol. /../ Der bør således være et klart skel mellem offentlige, private og kommercielle funktioner".

Udredningens privatkort er et sammenhængende værktøj til deltagelse i en fremtidig almindelig elektronisk kommunikation. Privatkortet er realisering af et mål om ét kort til teknisk identiske anvendelser. Spørgepanelet mente imidlertid, at kommercielle anvendelser skal findes på et eller flere andre kort end det offentlige borgerkort.

På den ene side kan man spørge, om denne vurdering går for vidt. Begrundelsen i slutdokumentet er dels, at banker m.v. øjensynlig ikke er interesseret i at betalingsfunktioner skal indgå i privatkortet og næppe kan tvinges; dels nogle vurderinger af sikkerheden. Begge vurderinger kan der stilles spørgsmålstegn ved. Finansrådet afviste for så vidt ikke privatkortet, men opstillede nogle kritiske overvejelser. Endvidere kunne man vel forestille sig at en udvikling mod et enkelt kort blev forbrugerdrevet - altså blev en realitet, hvis forbrugerne faktisk kræver det. Om den anden indvending må det siges, at privatkortet netop var skruet sammen, så der blev taget højde for et muligt problem med forskellig sikkerhedsnivoer i anvendelserne. Tager man derfor begrundelsen helt bogstaveligt kan den tilbagevises og det må derfor stadig overvejes om udredningens forslag til et enkelt privatkort ikke er den mest optimale løsning.

Men man kan *på den anden side* se panelets vurdering som udtryk for den principielle holdning, at den kommercielle verden og forholdet til offentlige myndigheder skal holdes adskilt. Men grænsen mellem hvad, der er kommercielt og hvad, der er offentligt er ikke så ligetil at fastlægge. Hvis et borgerkort f.eks. rummer mulighed for digital underskrift, kan det anvendes til at gennemføre betalinger i form af "digitale checks". Et Dankort kan anvendes som visuel legitimation overfor det offentlige. Hvis kommunikationsdelen ligger på bankernes betalingskort, ville den kunne anvendes til elektronisk aflevering af selvangivelse til skattevæsenet.

Panelet mener, at funktionerne digital underskrift og brevhemmelighed skal findes på borgerkortet. Men underskrift på elektronisk breve mv. kan også blive anvendt til varebestillinger, banktransaktioner og andre kommercielle formål. Det er endog her man kan forvente den mest udbredte brug af den digitale underskrift. Er det i strid med lægfolkenes egen vurdering, at kommercielle anvendelser ikke skal findes på borgerkortet? Panelet tager ikke direkte stilling til spørgsmålet. En løsning kunne være, at det kommercielle kort også har funktionerne digital signatur og brevhemmelighed. På den måde vil den enkelte kunne holde kommercielle anvendelser adskilt, men man kan også anvende borgerkortet til underskrive et kommercielt brev. Den praktiske forskel vil ligge i valgfriheden for borgeren i forhold til, hvilke kort man vil have, eller hvor og hvornår man vil anvende hvilket kort.

Den samlede vurdering må være, at der er behov for, at kravet om at adskille kommercielle og offentlige funktioner respekteres, omend på en pragmatisk måde. Det kunne gå ud på at etablere to kort - et kommercielt kort og et borgerkort.

I det følgende vil kun borgerkortet blive behandlet i dybden, da opstilling af krav til udformning af et egentligt kommercielt kort ikke har været formålet med projektet.

Kommercielt kort

Spørgepanelet anbefaler, at kommercielle virksomheder "udvikler et fælles kort". Denne vurdering må ses, som en reaktion på

det stigende antal betalingkort med tilhørende pin-koder, samtidig med at vi får stadig flere pin-koder til bruger-identifikation ved homebanking, homeshopping osv.

Betalingskort er i dag magnetstribekort. Når denne teknologi udskiftes med ic-kort bør denne teknologis muligheder udnyttes så forbrugerne har mulighed for kun at have ét kommercielt kort, som kan anvendes som betalingskort, til bruger-identifikation over for alle de virksomheder, banker o.l. man har et kundeforhold til, til at danne en digital signatur og etablere brevhemmelighed.

Borger ic-kort

Spørgepanelets vurderinger kan sammenfattes til et borger ic-kort med følgende funktioner. De enkelte anvendelser er beskrevet i afsnit 4.

Brugeridentifikation

- Adgang til offentlige edb-systemer, f.eks. egenservice hos kommune, AF eller statslige myndigheder.
Borgerkortet giver mulighed for udbygning af egenservice i den offentlige forvaltning. Spørgepanelet understreger, at der "på ingen måde må diskrimineres mod borgere, der vælger ikke at anskaffe et kort."
- Adgang til egne data i edb-registre (registerkontrol).
"Borgerne skal som minimum have adgang til egne registeroplysninger og mulighed for at følge myndighedernes anvendelse af disse data. Det vil indebære udvikling af en offentlig edb-service, der giver on-line adgang til offentlige registre og systemernes log-filer.
- Samtykke til videregivelse fra edb-registre (registerkontrol).
"Kortet skal indrettes, så indehaveren kan give samtykke til samkøring eller videregivelse af oplysninger". På konferencen - og i Datacentralens høringssvar - blev der gjort opmærksom på faren for at denne mulighed misbruges til at "tvinge" den enkelte til at udlevere oplysninger fra offentlige edb-registre. Denne risiko bør der tages højde for i den lovgivning, som danner grundlag for udstedelse af et borgerkort [67].
- adgangskontrol til egne (private) edb-systemer.

Digital underskrift

- krypterings-nøglepar, der gør det muligt at afgive en uafviselig digital underskrift.
"Der skal være mulighed for at underskrive elektroniske breve og dokumenter".

Brevhemmelighed

- kryptering af data, så elektroniske breve mv. ikke kan læses af uvedkommende.
"Det skal være muligt at opretholde brevhemmeligheden når man sender elektronisk post".
- kryptering af data på disketter og pc'ens harddisk.

Personlig legitimation

- manuel og automatisk personlig legitimation.
"Kortet med dets elektroniske del skal kunne bruges som legitimationskort over for offentlige myndigheder. Over for private må kun kortets visuelle del bruges."
"Private arbejdsgivere skal ikke kunne kræve, at medarbejderne anskaffer sig et borgerkort med henblik på elektroniske adgangskontrol".

Stamdata

- navn, adresse og personnummer på kortindehaver.
- mindreårige børns navn, adresse og personnummer.
"Om det skal rumme oplysninger om mindreårige børn, skal afklares nærmere. Blandt andet skal det undersøges, om børn kan få deres eget kort".

Spørgepanelet konkluderer entydigt, at et borger ic-kort "skal udstedes af en offentlig myndighed, og dets anvendelse reguleres af lovgivning".

Om den fysiske udformning skriver panelet, at der skal være "billede og underskrift på kortet". Der kan iøvrigt henvises til skitsen i afsnit 7.A d.

Et stykke infrastruktur

Borgerne vil sandsynligvis få flere forskellige kort, men de skal kunne benytte samme terminaler. Det må være et krav, at man

kan bruge samme udstyr i hjemmet, når der anvendes et offentlig selvbetjenings-system eller en privat serviceydelse. Selvom der vil blive tale om flere kort, bør det ske inden for fælles standarder, så der skabes et stykke infrastruktur. Der er i Danmark en - internationalt set - enestående erfaring med Dankort og DANMØNT for samlede kortsystemer, som indebærer en lang række fordele. Der må arbejdes for, at kommende kort, der reelt eller potentielt skal ud til alle danskere, også fungerer i alle systemer.

Biokode

Ic-kort teknologien giver mulighed for at anvende bio-kode til kortindehaver-identifikation. Ud fra sikkerhedsmæssige synspunkter giver bio-koden betydelige forbedringer fremfor de kendte pin-koder. Men er bio-koden social acceptabel? På grundlag af spørgepanelets vurdering er svaret ja. Det skal understreges, at en forudsætning for vurderingen af bio-koden i udredningen har været, at den digitaliserede værdi udelukkende findes i kortet og at man ikke kan gå fra denne værdi til det anvendte kendetegn (f.eks. fingeraftryk).

Det må derfor anbefales, at der arbejdes med at anvende bio-kode i forbindelse med ic-kort, der kræver en kortindehaver-identifikation.

En fremgangsmåde kunne være vedtagelse af en dansk standard, som vælger bio-kode og specificerer anvendelsen. En tidlig afklaring af, at bio-kode skal anvendes i fremtiden, vil gøre det muligt at udvikle kortlæsere (både selvstændige og sammenbyggede i telefoner, computere o.l), som kan anvendes til forskellige kort.

d) Forudsætninger for kortene

Spørgepanelet skriver i den samlede vurdering: "Borgerkortet synes, med de anvendelsesområder og begrænsninger, som vi har nævnt, ikke at have den store revolutionerende betydning, men vil formentlig heller ikke forpeste vores hverdag. Kortet berører ikke de væsentlige sider i vores liv og synes ikke at være af større betydning". På den baggrund vil det nok være rigtigst at sige, at lægfolkene kan acceptere kortet, men ikke egentlig anbefaler det. Denne accept og de ovenstående konklusioner bygger på en række forudsætninger, som skal uddybes.

Frivilligt

Borgerne skal have mulighed for at tage borger ic-kortet i anvendelse i takt med, at den enkelte oplever behov for det. Spørgepanelet formulerede dette centrale princip om frivillighed således: "Vi vil understrege at brugen af et eventuelt kort skal være frivilligt. Der må på ingen måde diskrimineres mod borgere, der vælger ikke at anskaffe et kort. Det bør sikres gennem lovgivning"

Det vil betyde, at der bør etableres dobbelte systemer, så man kan blive betjent både med og uden kort. Besparelserne for de, der ønsker at basere deres service på kortene - f.eks. det offentlige - vil altså ikke kunne indhentes med det samme, men vil komme efterhånden som fordelene ved kortene bliver synlige for befolkningen.

Ikke identitetskort

Spørgepanelet understregede, som omtalt ovenfor at borgerkortet ikke må blive et egentligt identitetskort.

I det etiske vurderings-kriterium: Frivillig personlig legitimation (afsnit 7.C g), spørges om man tør løbe risikoen for, at privatkortet anvendes til manuel og maskinel legitimation i en række situationer.

Et borger ic-kort kan anvendes til personlig legitimation og dermed fungere som et identitetskort. Det er derfor nødvendigt med en meget klar regulering af hvordan og i hvilke situation borgerkortet må anvendes til personlig legitimation. Der kan her henvises til bestemmelsen i lov om betalingskort §19: "Betalingskort må ikke kræves anvendt som legitimationsmiddel i andre sammenhænge end betalingstransaktioner med betalingskort og som hævekort"

Sikkerhed og brugbarhed

De høje krav til sikkerhed og brugbarhed (beskrevet i afsnit 5 og 6), som var en forudsætning for det foreslåede privatkort, er tilsvarende en forudsætning for det anbefalede borger ic-kort.

[66] Se f.eks. Public Interest Principles fra The Telecommmunications Policy Roundtable. Communication of The ACM January 1994/vol. 37 no. 1 s. 106.

[67] Se hertil bestemmelsen i forslag til EF-direktiv "om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger": ret til ikke at være tvunget til af en tredjemand - med mindre dennes krav bygger på national lovgivning eller fælleskabsretten - til at udøve sin ret til aktindsigt med henblik på at videregive sådanne oplysninger til denne tredjemand eller en anden person (artikel 14 stk. 1 litra 2).

Referencer

Generel litteratur om ic-kort m.v.

Roy Bright: Smart Cards: Principles, Practice, Applications (1988)

John McCrindle: Smart Cards.

M. Devargas: Smart Cards and Memory Cards. NCC (1992)

P.L Hawkes: Introduction to Integrated Circuit Cards, Tags and Tokens for Automatic Identification. I: P.L.Hawkes, D.W.Davies and W.L. Price: Integrated Circuit Cards, Tags and Tokens (1990)

John R. Parks: Automated Personal Identification Methods for Use with Smart Cards. I: P.L.Hawkes, D.W.Davies and W.L. Price: Integrated Circuit Cards, Tags and Tokens (1990)

Deltagere i arbejds-sessioner

Sikkerhedsspørgsmål er behandlet på et scenarie-studie med deltagelse af: Direktør Jan Carlsen, Institut for Datasikkerhed; direktør, lektor Peter Landrock, Cryptomathic; konsulent Leif Kjøller, Danmønt; konsulent Preben Rahtgen, PBS og særlig sagkyndig i Dansk Standard S142u17 (identitets og kreditkort); edb-sikkerhedschef Ole Stampe Rasmussen, PBS.

Tekniske muligheder for indførelse af et borger ic-kort er behandlet på et seminar med deltagelse af: Udviklingschef Jens Linboe-Larsen, DANMØNT; konsulent Ole Lachmann, Dansk Udviklings Service; civ.ing.lic.tech Thomas Skousen, Fischer & Lorenz.

Etiske og retssikkerhedsspørgsmål er behandlet på et seminar med deltagelse af: prof.dr.theol Sven Andersen, Århus Universitet; prof.dr.jur Peter Blume, Københavns Universitet; lektor datalog Hasse Clausen, Datalogisk Institut Kbh. Universitet; lektor cand.jur. Oluf Jørgensen, Aalborg Universitetscenter.

Interessent-gruppen

Finansministeriet, APD
Indenrigsministeriet, CPR-kontoret
Amtsrådsforeningen
Kommunernes Landsforening
Forbrugerrådet
Socialrådgiverforeningen
COII
HK
Praktiserende Lægers Organisation
Kommunedata
DataCentralen
Dansk Standard
Dansk Standard S142u17(Identitetskort)

22.12.97 Teknologirådet tekno@tekno.dk