Søker: **Tage Stabell-Kulø**
Vesterliveien 30
9013 Tromsø

Oppfinner: Søkeren

Oppfinnelsens benevnelse: Sikkert kort med kommunikasjonskanal til brukeren

-1-

Datamaskiner kan produseres i en størrelse som gjør det mulig å inkludere en maskin på et kort noen få millimeter tykt. En typisk anvendelse av denne velkjente teknologien benyttes i de populære smartkortene. Oppfinnelsen angår en forbedring av denne teknologien (ikke begrenset til smartkort), slik at datamaskinen på kortene kan brukes til å generere sikre digitale signaturer.

De aller fleste av smartkortets egenskaper er standardiserte i standarden "ISO/IEC 7810 Identification cards – Physical characteristic" og "ISO/IEC 7816: Identification cards – Integrated circuit(s) cards with contacts" med tilhørende dokumenter. Standarden er utgitt av *International Organization for Standardization (ISO), Technical committee / subcommittee: JTC 1/SC 17 (Identification cards and related devices), International Organization for Standardization (ISO), 1 rue de Varembé, Case postale 56, CH-1211 Genève 20, Sveits*. I Norge kan disse standardene skaffes fra *Norges Standardiseringsforbund, Postboks 353 Skøyen, 0213 Oslo*. Kortenes mekaniske og elektriske egenskaper, samt protokoller for utveksling av data, er beskrevet i stor detalj.

Enheter for å kommunisere med smartkort kalles en *smartkortlese* eller bare *leser* når det fremgår av sammenhengen hva det siktes til. En leser er en mekanisk enhet i hvilken man kan plassere et smartkort slik at kortets elektriske kontakter forbindes med en datamaskin. Denne maskinen kan enten befinne seg i leseren, eller være forbundet med leseren via elektriske kabler. Leseren gjør det altså mulig for datamaskinen på kortet å kommunisere med andre datamaskiner; elektroniske betalingssystemer er en typisk anvendelse.

En utfyllende beskrivelse av smartkortteknologi og lesere kan man finne i boken “Smart Cards – A Guide to Building and Managing Smart Card Applications” av Dreifus og Monk, IEEE Computer Press 1997, ISBN 0-471-15748-1.

Av særlig intresse er at det når smartkort produseres på en tilfredstillende måte har de den egenskap at de data som er oppbevart inne i kortets elektronikk er *meget* godt beskyttet. Det vil si, det er ikke praktisk mulig å hente ut de data som er plassert i kortet uten å kommunisere med programvaren som også lagres på kortet. I særdeleshet, kortene kan brukes til å oppbevare krypteringsnøkler,

Krypteringsnøkler kan, blant annet, brukes til å produsere *digitale signaturer*. Digitale signaturer har en lang rekke anvendelser innen elektronisk handel, elektronisk post, og så videre. Som regel forutsettes det at for at en digital signatur skal ha noen mening, må krypteringsnøkkelen som benyttes være hemmlig (for alle andre enn den som genererer signaturen). En fyllestgjørende presentasjon av kryptografisk teknologi finner man, for eksempel, i boken “Handbook of applied cryptography” av Meneze, van Oorschot og Vanstone, CRC Press 1997, ISBN 0-8493-8523-7.

I mange henseende er smartkort et idéellt sted å oppbevare krypteringsnøkler. Dersom kortet utstyres med støttefunksjoner for å beregne slike signaturer behøver heller ikke nøkkelen forlate kortet eftersom signaturen kan i sin helhet genereres på kortet. Slike kort er tilgjengelige fra mange produsenter.

Rent praktisk genereres en signatur på et stykke data ved at et smartkort settes inn i en leser, de data som skal signeres (eller en transformasjon av disse) overføres til kortet, datamaskinen på kortet genererer signaturen, hvoretter signaturen leveres fra kortet tilbake til leseren. Denne fremgangsmåten avslører en viktig svakhet ved bruken av smartkort. Problemet er at brukeren

ikke har noen mulighet for å "se" hvilke data som signeres. Det vil si, leseren kan fortelle brukeren (via en skjerm, for eksempel) at følgende tekst vil bli overført til kortet for signering: "Send 10 kroner til Svindel AS", mens leseren i virkeligheten overfører: "Send 1.000 kroner til Bedrag AS". Årsaken til at det er mulig å "lure" smartkortet til å signere noe som ikke skulle ha vært signert er at smartkortet ikke kan kommunisere med brukeren uten å gå gjennom kortleseren, som i denne sammenheng ikke er til å stole på. Det design smartkort har gjør altså at sikre digitale signaturer — sikker i den forstand at brukeren vet hva som faktisk ble signert — ikke er mulig.

Smartkort kan også benyttes til andre formål, for eksempel å autentisere brukere. Autentisering kan realiseres, for eksempel, ved at brukeren utstyres med et smartkort og en hemmelig kode. Nå skjer autentisering ved at brukeren både må presentere kortet i en leser og samtidig presentere sin hemmelige kode (ofte kalt PIN-kode). Man har en kombinasjon av noe brukeren *har* (kortet) og noe brukeren *vet* (koden). Problemet er, igjen, at brukeren ikke kan kommunisere direkte med kortet. Den hemmelige koden må overleveres til leseren, som i denne sammenheng ikke er til å stole på. Dagens minibanker og betalingsterminaler i alle norske butikker fungerer på denne måten.

Løsningen på dette *kunne være* å produsere smartkortene slik at det har et medium for å kommunisere med brukeren (for eksempel en liten skjerm; i det videre bruker vi ordet skjerm for å illustrere dette mediet) og et medium for å motta informasjon fra brukeren (for eksempel et tastatur eller en fingeravtrykkleser; i det videre bruker vi ordet tastatur for å illustrere dette mediet) på motsatt side av de elektriske kontaktene; kontaktenes plassering er gitt av standarden. Nå kunne kortet informere brukeren om hva som skal signeres, og brukeren gi sitt samtykke. Hvordan dette kan gjøres i teorien er beskrevet i artikkelen "Authentication and Delegation with Smart-cards"

av Abadi, Burrows, Kaufman og Lampson, publisert i “Science of Computer Programming” volum 21 nummer 2 (oktober 1993) sidene 93 til 113. I eksemplet med autentisering kunne man, for eksempel, be brukeren skrive sin hemmelige kode på tastaturet eller legge en finger på fingeravtrykkleseren, og la kortet kommunisere med leseren.

Denne type løsninger, som fungerer i teorien, lar seg imidlertid ikke uten videre realisere. Problemet er at kortet må kunne stå (delvis) inne i leseren for å kunne kommunisere, slik det er beskrevet i standarden. I essens, problemet er: Hvordan produsere et kort som har smartkortes fordeler, men ikke dets ulemper.

Det hele grunner seg i at (datamaskinen på) kortet ikke har noen mulighet til å kommunisere med brukeren mens kortet står inne i leseren. Dette lar seg løse, i henhold til oppfinnelsen, ved at man lager et hengslet kort som er slik at ene delen av kortet er vendt mot brukeren samtidig som den andre delen står inne i kortleseren.

-2-

I det videre vil vi benytte ordet “smartkort” for å illustrere et kort, produsert i for eksempel et plastmateriale, som inneholder en prosessor, og som har elektriske kontakter. Vanligvis benyttes ordet ene og alene for å beskrive de kortene som følger standarden nevnt over, men vi vil bruke ordet i en noe videre forstand til å inkludere kort som kan være mindre, større, tykkere eller tynnere. Eller som ikke har samme fysiske egenskaper (tåler høyere temperatur, for eksempel).

Med *Sikkert kort med kommunikasjonskanal til brukeren* ifølge oppfinnelsen blir det mulig å produsere et kort som gjør det mulig med kommunikasjon

mellom kortet og brukeren. I tillegg kan man, om man ønsker, lage et kort som følger de standarder som gjelder for smartkort, samtidig som kortene kan utstyres med både en skjerm og med et tastatur som beskrevet overfor.

Dette oppnås i følge oppfinnelsen i korthet ved at den delen av kortet som inneholder kortets elektriske kontakter hengsles på resten av kortet, slik at det får en "flapp" (2) som vist på figur 1; på denne figuren er flappen "nede". Denne "flappen" utgjør kortets minste del, mens resten utgjør kortets største del. Kortets minste del henger fast i resten av kortet med en hengsel (1). Elektriske ledere forbinder prosessoren (som vanligvis vanligvis befinner seg under kontaktene (3)) med tastaturet og skjermen gjennom hengslet (1), slik at programmer som kjører på prosessoren kan lese fra tastaturet og skrive på skjermen. Figur 2 viser kortet sett fra siden, med flappen "oppe". En tilhørende kortleser kan nå konstrueres slik at hoveddelen av kortet blir liggende mot leseren med flappen inne i leseren.

Når kortet skal benyttes, stikkes flappen på kortet (2) inn i en sprekk i leseren og skyves inn. Skjermen på kortet kan nå leses av brukeren, samtidig som leseren gir støtte for kortet slik at tastaturet på kortet kan betjenes, samtidig som kortets elektriske kontakter (3) er i kontakt med leserens elektriske kontakter. De teoretiske betraktninger som ble gjort i artikkelen av Abadi, Burrows, Kaufman og Lampson (nevnt over) kommer nå til anvendelse eftersom brukeren kan kommunisere med kortet på en tilfredstillende måte. For eksempel kan digitale signaturer genereres, eller kortet kan verifisere at brukeren kjenner en hemmelig kode, eller kortet kan kreve at brukeren plasserer en finger på en fingeravtrykkleser.

Det presiseres at det i følge oppfinnelsen ikke er gjort begrensninger knyttet til de standardiserte smartkortene. Det vil si, kortet i henhold til oppfinnelsen kan produseres med fysiske mål helt uavhengig av de standardiserte

kortene. Men man kan, i følge oppfinnelsen, velge å følge standarden.

Videre, figurene viser en realisering av oppfinnelsen hvor hengselen (1) er plassert omlag halveis i kortets lengderetning. Dette er ene og alene et eksempel; hengselen kan plasseres hvor som helst i lengderetningen. I særdeleshet: Om hengselen plasseres i kortets ende, blir "flappen" (2) like lang som resten av kortet. Kortet kan da produseres slik at flappen helt og holdent følger standarden for smartkort.

Det på figur 1 inntegnede tastatur og skjerm er kun eksempel på mulige kommunikasjkonskanaler mellom kortet og brukeren. Biometriske enheter (fingeravtrykklesere eller liknende) er andre mulig kanaler for kommunikasjon fra brukeren til kortet. Blinkende dioder er et mulig eksempel på kanal fra kortet til brukeren.

Hengselen (1) skal produseres av et ikke angitt materiale.

Figur 1 viser hvorledes "flappen" i utfoldet stilling står normal (vinkelrett) på resten av kortet. Dette er ene og alene for å gjøre illustrasjonene lette å forstå. Den maksimale åpning av "flappen" kan godt være mindre eller større enn $90°$.

Kortet skal produseres i et ikke angitt materiale.

-3-

Patentkrav

1. *Sikkert kort med kommunikasjonskanal til brukeren*, karakterisert ved et kort som er utstyrt med en kommunikasjonskanal fra brukeren til

kortet og en kommunikasjonskanal fra kortet til brukeren, og en hengsel (1) som gjør at delen av kortet med de elektriske kontaktene (3) er hengslet på resten av kortet.

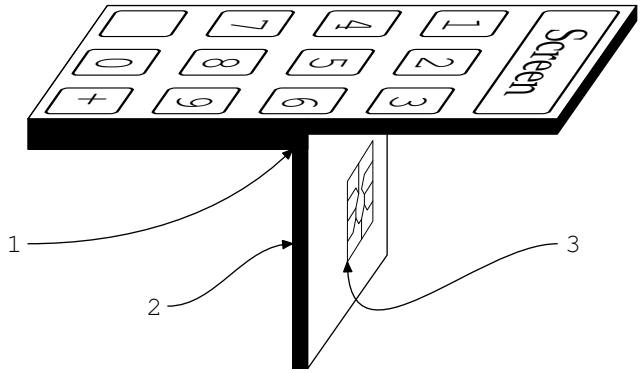
2. *Sikkert kort med kommunikasjonskanal til brukeren* i følge krav 1, karakterisert ved at prosessoren i kortet har kontakt med kommunikasjonskanalene mot brukeren og kortets elektriske kontakter (3) gjennom elektriske ledere som passerer gjennom hengselen (1).

3. *Sikkert kort med kommunikasjonskanal til brukeren* i følge krav 1–2, karakterisert ved at kortets elektriske kontakter (3) er plassert på "flappen" (2) som oppstår fordi kortet er utstyrt med en hengsel (1).

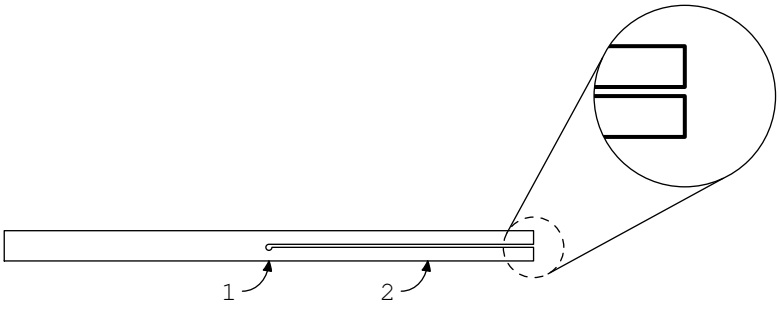
-4-

Sammendrag

Sikkert kort med kommunikasjonskanal til brukeren gjør kommunikasjon mellom kortet og brukeren mulig, samtidig som kortet kan kommunisere med en kortleser. Dette muliggjør, blant annet, digitale signaturer hvor brukeren kan verifisere det som skal signeres. Kortet er utstyrt med en kommunikasjonskanal fra brukeren til kortet, realisert for eksempel som et tastatur, og en kommunikasjonskanal fra kortet til brukeren, for eksempel en skjerm, slik at delen (2) med kortets elektriske kontakter (3) er hengslet (1) til resten av kortet. Resten av kortet inneholder kommunikasjonskanalene (vist som et tastatur og en skjerm). En tilpasset kortleser kan nå produseres slik at kortets minste del (2) stikkes inn.



Figur 1:



Figur 2: