

Cashcards

En studie av tekniken och användandet
av cashcards.

Sammanfattning

Den här rapporten beskriver inledande historia och ekonomiska aspekter kring cashcards. Sedan behandlas systemet som en helhet och hur man praktiskt använder cashcards. Därefter redovisas tekniken i den processor som sitter i kortet och hur en laddningsstation är uppbyggd. Dessa avsnitt är tekniskt avancerade. Rapporten är av beskrivande karaktär och därför dras ej några direkta slutsatser.

SAMMANFATTNING.....	2
INLEDNING.....	4
SYFTE.....	4
FRÅGESTÄLLNINGAR.....	4
HISTORIK.....	5
EKONOMISKA ASPEKTER HOS CASHCARDSYSTEMET.....	5
CASHARD I FRAMTIDEN.....	7
SYSTEMÖVERSIKT.....	8
KONTANTKORTET.....	8
BETALNING MED KORTET.....	9
BETALTERMINALEN.....	9
LADDNINGSTERMINALEN.....	9
DATAÖVERFÖRING TILL BANK.....	9
SMARTA KORT OCH ANDRA KORT.....	9
IC-MINNESKORT.....	10
SMARTA KORT.....	11
KONTAKT !.....	11
SMARTA KORTETS MINNE.....	13
CPU OCH OPERATIVSYSTEM.....	14
TILLVERKNING AV ETT SMART KORT.....	14
DATAÖVERFÖRING.....	16
SÄKERHET.....	16
Kryptering	16
Symmetriska algoritmer.....	17
Asymmetriska algoritmer.....	17
Transaktionsnycklar.....	17
TEKNIK HOS CASHCARD.....	17
CASHLOAD DEVICE.....	18
HÅRDVARA.....	18
MJUKVARA.....	18
SYSTEMSÄKERHET.....	19
INFORMATIONÖVERFÖRING.....	19
<i>Format</i>	19
<i>Informationsflödet</i>	20
AVSLUTNING.....	23
REFERENSER.....	24

Inledning

I rapporten får läsaren en översikt av cashcardsystemet i Sverige.

De frågor som besvaras är bl a vad det finns för nytta med cashcards och hur tekniken bakom systemet ser ut. Under rubrikerna Historik och Cashcard i framtiden tas ursprunget till tekniken och till vad den kan leda upp. Vidare behandlas den tekniska sidan av microprocessorn och laddningsstationen grundligt. För att kunna redogöra för laddningsstationens funktionalitet har ICL Financial Terminals konsulterats och det har varit till stor hjälp.

Syfte

Den här rapporten är en del av kursen TDDB31, Orientering i IT-infrastukturer. Ämnet är valt med tanke på dess aktualitet och att det ligger en intressant teknik bakom systemet. Rapporten kan läsas av alla som är intresserade av cashcardsystemet och den bakomliggande tekniken. För att till fullo tillgodogöra sig rapporten bör dock läsaren ha grundläggande datakunskaper.

Frågeställningar

I rapporten skall vi försöka besvara några frågor:

- Vad finns det för olika nyttor med cashcards?
- Hur fungerar det praktiskt?
- Hur fungerar kortets teknik?
- Hur är laddningsterminalen uppbyggd?
- Vad kostar systemet och vem tjänar på det?

Historik

Här följer en kort historik bakom det system för cashcard som idag finns i Sverige.

Cashsystemet startade på försök i Uppsala och Halmstad i november 1996. Idag finns det femton orter i landet; bl.a. i Norrköping för att nämna närmast belägna plats. En rikslansering av cash inleddes i år med start i Stockholm och i framtiden är det tänkt att man ska kunna använda cash även utomlands med flera valutor samtidigt, se vidare under kapitlet om framtiden. Själva tekniken med s.k. smarta kort är däremot ingen nyhet. Redan 1974 tog en fransman vid namn Roland Moreno patent på smarta kortet. Det skiljer dock en hel del i den teknik som används idag, vilket inte är någon större överraskning. Den första tillämpningen av smarta kort som började att användas var telefonkort som är en enkel form av smarta kort. 1985 introducerades dessa i Frankrike och sedermera även i Sverige. Telefonkortet innehåller endast en mindre minneskrets för att hålla reda på hur många markeringar som kortet har kvar och kan jämföras med vanliga kort med magnetremsa. Om man däremot tittar på de smarta kort som lanseras idag, som t.ex. cashcarden så är de små miniatyrdatorer med processor, minne operativsystem och program.

Omsättningen för cashcarden var under 1997 63 miljoner kronor och det skedde ca 980 000 transaktioner och sedan starten har inköp för ca 100 miljoner kronor gjorts med cashcard. Det finns ungefär 5200 köpställen och 120 000 cashcard i Sverige idag. Det var sparbanken som var först ut på den svenska marknaden med småskaliga testkörningar i Lund 1995-96. Den första större satsningen kom i mars 1996 då ett avtal mellan dåvarande sparbanken och nordbanken ingick ett samarbetsavtal. För att skapa en gemensam teknisk standard valde man det s.k. Protonsystemet som kommer från det bankägda dataföretaget Banksys i Belgien och idag används i flera länder i Europa. Protonsystemet anpassades sedan till den svenska marknaden före det implementerades. SE-Banken anslöt sig sedan till samarbetet i augusti samma år.

Ekonomiska aspekter hos Cashcardsystemet

Idag finns flera olika betalningsmedel där kontanter och kontokort är de mest förekommande. Andra exempel är checkar och bank- och postgiro eller motsvarande överföringar. Cashcardsystemet är tänkt att bli ett bra komplement till de två förstnämnda betalningsmedlen. Det kommer även att vidga möjligheterna för användandet av kort istället för kontanter på ställen där det i dag inte lönar sig att använda sig av kontokort eller där hantering av kontanter inte riktigt uppfyller önskvärda krav på säkerhet och lönsamhet. Det kommer inte att kunna fungera som ett rent substitut gentemot kontanter eller kontokort då det har en övre gräns för det belopp som är möjligt att ladda kortet med.

Detta avsnitt avser att avhandla de fördelar som Cashcard systemet har som komplement till kontanter och kontokort i den dagliga handeln samt även ge exempel på vissa områden där systemet kommer att kunna ge helt nya möjligheter som ett substitut. Om så finnes skall det även försöka peka på vissa nackdelar. Dessa fördelar kommer främst att belysas ur ett rent ekonomiskt perspektiv men även andra fördelar kommer att lyftas fram såsom miljö och hygien. Säkerhetsaspekter kommer också att belysas eftersom dessa direkt kommer att utgöra ekonomiska fördelar.

Systemet har många fördelar både för handeln och för kunderna. Som snart kommer att synas ligger de flesta fördelarna i jämförelsen med kontanter som betalningsmedel.

Med början i handeln så finns en stor fördel i det att Cashcard sparar tid vid betalning vilket ger snabbare och billigare betalningsrutiner. Eftersom det inte krävs någon PIN-kod utan bara en enkel bekräftelse så går det betydligt snabbare än vid kontant betalning. Man sparar även in tid gentemot kontokorts betalning eftersom allting lagras offline till skillnad mot den uppringning och kontroll gentemot en bank som sker då man handlar med kontokort. När dagen är slut så sparas en hel del dyrbar arbetstid in som annars går till att räkna ihop kassorna samt transportera pengarna till banken tack vare den enkla överföringsmekanismen mellan handlaren och banken som tidigare nämnts. En undersökning gjord av Handels Utredningsinstitut på uppdrag av sparbanken ger att en kontant betalning i genomsnitt tar 24 sekunder att jämföra med 10 sekunder i genomsnitt för cashcardet. Dessa tider innefattar det efterarbete som nyss nämnts. Enligt undersökningen så medför detta att kostnaden för en kontantbetalning blir 1.06 kr emedan kostnaden för en cashcardbetalning stannar på 0.46 kr. Detta är mindre än halva kostnaden. De snabbare betalningsrutinerna minskar köerna vilket gör handeln mer attraktiv och handlaren kan hinna mer fler kunder. Eftersom beloppet alltid är exakt så kommer man även ifrån, felräkningar i kassan vilket sparar pengar.

Cash öppnar nya möjligheter på inköpsställen där det inte tidigare var aktuellt med kortköp, t.ex. kiosker, biografier eller andra ställen där inköpssummorna är så låga att kontokortsköp inte har varit lönsamt eller aktuellt. Ytterligare en fördel är det att man nu kan komma runt många av de problem som föreligger vid obemannade inköpsstationer såsom parkerings- eller varuautomater. Som kund slipper man att man alltid måste ha jämna kontanter. Handlaren slipper kostnader för tömning och dessutom kommer det bli möjligt att, eftersom automaterna kommer att anslutas i ett nätverk, läsa av när automaten är tom eller om tekniska fel uppstår. Kostnader minskar och man kan lättare undgå att maskinen står tom under vissa perioder. Cash kommer att öka säkerheten för handlaren eftersom man minimerar möjligheter att komma över kontanter vid butiksrån eller stöld av automater. Som kortinnehavare kan man spärra kortet om man skulle bli av med det och kortet blir därmed obrukbart. Ett förlorat kort innebär inte förlorade pengar. Cashkortet är gjort av återvinningsbar PET-plast som tjänar miljön och dessutom är det en fördel ur allergisynpunkt ty de som har nickelallergi slipper problem och dessutom är hantering av mynt och sedlar mindre hygienisk.

Cashkortet gör det möjligt att alltid ha tillgång till pengar för alla möjliga typer av inköp. Både stora och små. Särskilt om det kombineras med ett vanligt kontokort för de lite större inköpen. Detta kommer att kunna ge vissa samhällsekonomiska fördelar eftersom konsumtionsmöjligheterna förbättras samtidigt som handlarens lönsamhet kan ökas.

De stora ekonomiska vinsterna kommer dock att tillfalla bankerna i och att man i förlängningen kommer att undvika att det finns ekonomiska medel i händerna på konsumenterna. Det medför billigare hantering och framför allt så kan ju banken lyfta ränta på de pengar som fingerat ligger på kundens kort men som i verkligheten ligger på bankens depå till dess att kunden spenderar dem. Bankerna kommer att få en allt större tillgång till ekonomiska resurser för investering och utlåning och erhåller stora möjligheter att öka sina vinster. Pengar kommer endast att, i begränsad mängd, finnas i

betalterminaler i handeln under dagen medan resterande finns tillgängligt för bankerna. (Dvs ränta kommer att till falla dem.)

Cashard i Framtiden

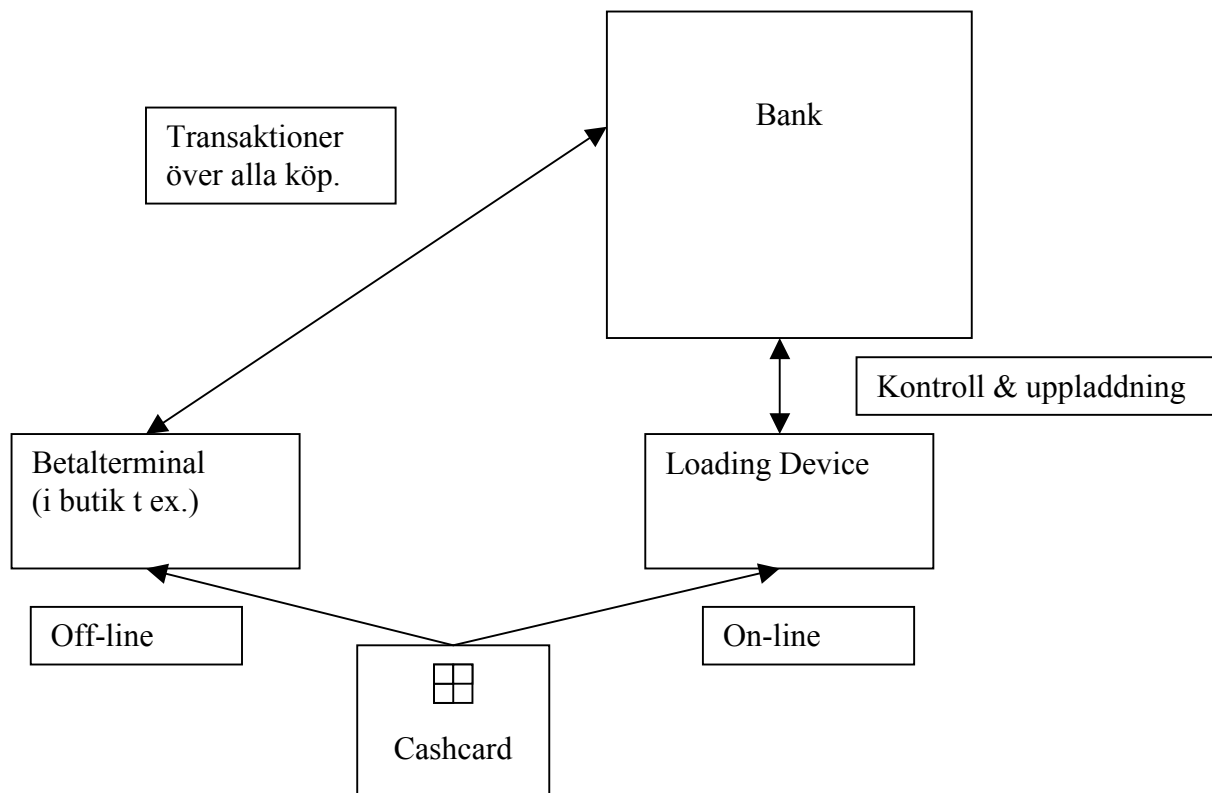
Cashcardet har ett chip med stor lagringskapacitet. Detta ger cash hög potential för framtida förbättringar. Här finns ju gott om plats för annat än bara lagring av pengar att konsumera. Cash kortet är ett så kallat smart kort som nämnts tidigare och i microprocessorn, ”chipet”, finns lagringsutrymme för ca 64 000 tecken. Här kan tänkas att man kan komma att kunna lagra en mängd olika typer av information. Kortet kan tänkas komma att användas som medlemskort, lånekort av olika slag samtidigt som det kan innehålla ägarens ID-handlingar och annan viktig information om kortägaren. Om man gör en direkt jämförelse med ett magnetkort så kan ett smart kort lagra upptill 80 ggr mer information och är dessutom mycket säkrare och svårare att förfalska. Man kommer alltså att kunna använda samma kort till en mängd olika aktiviteter i framtiden såsom nyckelkort och inloggning till Internetbanker samt på bussen eller som medlemskort på ”gymmet” vilket är en smakfull lösning på dagens stora mängd av olika plastkort och lappar med koder och lösenord som skall rymmas i plånboken eller i ens minne.

Eftersom man i Sverige har valt Protons systemet som används i andra europeiska länder finns stor potential för ett framtida internationellt användande. Systemet har dessutom kapacitet att kunna ladda korten med olika valutor. Det svenska systemet är dessutom ett öppet system som innebär att ytterligare banker kan ansluta sig till systemet så det finns stora utvecklingsmöjligheter. Möjligheten för en internationell standardisering är väldigt viktig, särskilt med tanke på införandet av ett införandet av Euro som en europeisk valutaunion.

En ytterligare framtida applikation är faciliteten med en s.k. hemladdare där man kan ladda sitt kort från hemmet via en reguljär Internet-uppkoppling. Man kommer på sätt att ha tillgång till en egen bankomat i hemmet. Utifrån detta kan ju tycka att det finns stor potential för att cashcard-systemet kommer att bli en stor tillgång för människan i framtiden, vilket nog är precis vad det handlar om...

Systemöversikt

I det här avsnittet följer en praktisk översikt av systemet. För tekniska detaljer hänvisas till senare kapitel.



Schematisk bild över systemets kommunikation

Cashcardet är av den typ av IC-kort (Integrated Circuit) som kallas kontaktkort. Det som är kännetecknande för kontaktkortet, i motsats till betalkort, är att köpet sker off-line och det behövs heller ingen PIN-kod för att utföra köpet. Detta är möjligt genom att i betaltterminalerna lagras alla köp. Att ladda kortet kan direkt jämföras med att gå till Minuten eller Bankomaten. Laddaren har on-line kontakt med banken och här använder man sin PIN-kod för att ladda kortet men pengar.

Kontaktkortet

Kortets kärna är en mikroprocessor som lagrar information. Processorn kan lagra upp till 128 kbyte, och det innebär att användningsområdena för kortet är väldigt stora. Mikroprocessorn är bara åtkomlig via en betal- eller laddningsterminal, och det gör att säkerheten är mycket hög. Detta innebär att det praktiskt taget är omöjligt att manipulera med den data som finns lagrad. Se detta i motsats till kort med magnetremsa som är mycket lätt att kopiera. Kortets livstid, > 10 år, är betydligt längre än ett magnetremsekort, ≈ 2-3 år. Mer om kortets teknik följer nedan.

Betalning med kortet

För att genomföra ett köp med kortet krävs att det är laddat med kontanter och att affären har en betalterminal. Betalningen går till så att kunden sätter kortet i betalterminalen och genom att godkänna summan med ett tryck på en OK-knapp dras beloppet från kortet. Summan lagras i betalterminalen och vid dagens slut kopplas den upp mot bankens dator och den sammanlagda summan överförs från banken till butikens konto. På så sätt hanteras inga kontanter och medföljande problem elimineras. För små köp krävs ingen PIN-kod, men vid köp med större summor används denna, likaså om man gör många köp under kort tid så får man efter ett antal köp ange sin kod. Detta för att öka säkerheten. Undersökningar har visat att ett kontantköp tar i snitt 24 sekunder och ett köp med cashcard i snitt 10 sekunder. I beräkningen ingår då hantering av kontanter samt tömning och räkning av kassan. Kostnaden för kontantkort ligger på 1,06 kr/köp och med cashcard 0,46 kr/köp.

Betalterminalen

Betalterminalen innehåller en kortläsare, där kundens kort avläses, köpeskillingen dras av och det nya saldot registreras. För att systemet skall vara säkert finns två säkerhetsfunktioner, CSM och SAM, implementerade. Alla köp sker off-line, och vid dagens slut kopplas terminalen upp mot bankens dator och alla transaktioner kontrolleras och köpesumman överförs till butikens konto.

Laddningsterminalen

När kunden skall ladda sitt kort besöker han/hon en laddningsterminal. Proceduren är liknande dagens Minuten och Bankomater, det som skiljer är att det finns betydligt fler laddningsterminaler än Minuten. Det tar ungefär 35-40 sekunder att ladda kortet idag, men ICL jobbar på lösningar för att komma ner mot 20 sekunder. Det maximala beloppet som går att ladda är idag 1500 kr och minimum är 50 kr.

Dataöverföring till bank

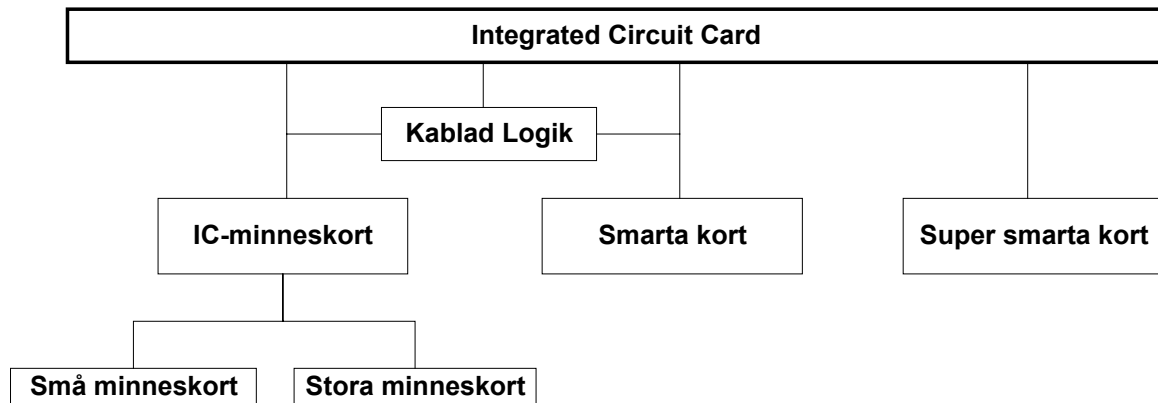
När kortet laddas eller när en betalterminal skall tömmas sker det via det vanliga telefonnätet. Informationen krypteras av säkerhetsskäl.

Smarta kort och andra kort

Här följer en studie av tekniken hos olika typer av IC-kort och en djupare granskning av främst smarta kort.

De kort som har någon form av elektronisk krets inbyggd kallas vanligen för *Integrated Circuit Cards* – IC-kort. Det finns många undergrupper till IC-kort och efter att de vanligaste typerna nämnts så presenteras smarta kort mer ingående. Bergdahl¹ schematiserar familjen av IC-kort så här:

¹ Bergdahl Tekn. Attache....

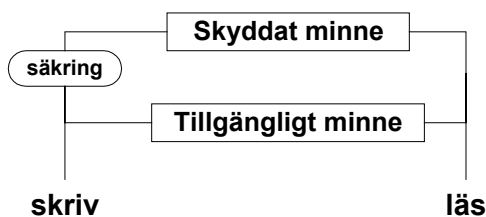


IC-minneskort

När det gäller IC-minneskort kan det skilja mycket i minneskapacitet, därav indelningen. Vissa IC-minneskort har kablad logik, andra inte. Vidare delas små minneskort upp i seriella och skyddade kort.

De seriella korten är utan kablad logik och kan inget annat än att passivt läsa och skriva information. Till funktion så är de lika kort med magnetremsor och det går att fritt skriva och läsa information från kortet om man har hårdvara som passar.

Skyddade kort är säkrare än seriella kort eftersom de skyddar delar av kortets minne. Viss information, som t ex ett serienummer, skrivs vid kortets fabrikation in i det skyddade minnet. Därefter påför man kortet en spänning som är tillräckligt hög för att den ska bränna av säkringen. Ingenting kan nu skrivas eller ändras i det skyddade minnet.



IC-kort med skyddat minne.

De skyddade korten innehåller även kablad logik i minnet vilket gör att minnets tillgänglighet kan kontrolleras och sättas i samband med exempelvis ett lösenord som hårdvaran känner till. Denna typ av kort som ofta kallas *Chip Card* används i stor skala av bl a France Telecom i telefonkort.

PC-kort, t ex den amerikanska standarden PCMCIA, är exempel på stora IC-minneskort. Kortet används ofta tillsammans med bärbara datorer och olika typer av kort kan fungera bl a som kommunikationskort och minneskort.

Smarta kort

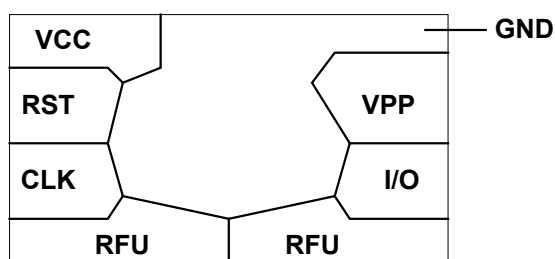
Efter att snabbt ha berört IC-minneskort så skall nu smarta kort granskas närmare. Enligt gällande ISO-standard så är storleken på kortet 85 mm x 53 mm och tjockleken är 0,76mm. Kortet gör vanligtvis i PVS- eller ABS-plast.

Orsaken till att de kallas smarta är att de har en inbyggd mikroprocessor som gör det möjligt för kortet att processa data. Försök med kort som har två inbyggda processorer har gjorts men fortfarande är korten som har en processor vanligast. Kort som dessutom har en display och ett tangentbord brukar kallas supersmarta kort. De supersmarta korten behöver inte vara särskilt mycket större än andra IC-kort men vad som hindrat dess spridning är den avancerade tekniken är ganska kostsam.

Det finns tre typer av smarta kort; **kontaktkort**, **kontaktlösa kort** och **proximity-kort**. Kontaktkort kräver fysisk kontakt mellan kortet och kort-läsare/skrivare, vanligtvis kallad CAD². Kontaktlösa kort utnyttjar induktion och kapacitiv teknik och kräver inte direkt kontakt. Dock måste kortet placeras mycket nära CAD och i rätt riktning i förhållande till denna. Proximity-kort är kontaktlösa kort med en längre räckvidd. De kallas ibland för passiva kort och aktiveras när det kommer i närheten av CAD. Läsning och skrivning kan ske på ett avstånd upp till 0,5 m. Proximity-kortet kommunicerar via radiofrekvens eller med laserteknik. För att kunna kommunicera så krävs självklart en strömförsörjning för kortet. Denna kan utgöras av mottagen magnetisk energi eller ett i kortet inbyggt batteri. Proximity-korten har en krävande teknik, är ofta tjockare än andra smarta kort och slutar att fungera när batteriet tagit slut. Å andra sidan så finns det klara fördelar med den kontaktlösa kommunikationen, exempelvis i samband med kollektivtrafik där det krävs hög genomsläppshastighet.

Kontakt !

Kontaktkorten är allra vanligast. På kortets ena sida syns en samling kontaktbleck under vilka en modul innehållande mikroprocessorchipet finns. Via kontaktblecken sker kommunikation med CAD och även strömförsörjningen. För kontaktkort finns en



utarbetad standard – ISO 7816 – och den definierar bl a de olika kontaktblecken. Enligt standarden, ISO 7816-2, så finns åtta bleck men endast sex används för kortets kommunikation med omvärlden.

De av ISO 7816-2 definierade kontaktblecken.

Arbetsspänning, VCC

Kortets arbetsspänning (VCC) är definierad till att vara mellan 4,75 och 5,25 volt där den maximala strömförbrukningen av 200mA. Tekniken går dock mot att lägre

² CAD – Card Acceptor Device; exempelvis en kortläsare eller en laddare.

spänning, 3 volt, skall användas tillsammans med nya typer av halvledare som kräver allt mindre strömförsörjning. En strömförbrukning på 200mA är väl högt för dagens teknik och de flesta smarta kort har en förbrukning på endast 10mA till 20 mA. ETSI³ har i sina standardiseringar satt den maximala strömförbrukningen till 20mA vid normalt användande och när det gäller *sleep mode*, där kortet är inaktivt fränsett att det förser volatila minnen med den ström de behöver för att bevara sin information, så är den maximala strömförbrukningen 200

Jord, GND

GND är jordreferens till arbetsspänningens potential.

Återställning, RST

Återställningssignalen används för att starta upp de program som finns i det smarta kortets ROM. Enligt ISO-standard så finns tre återställningstyper: *internal reset*, *active low reset* och *synchronous high active reset*. De flesta kort idag använder *active low reset* som återställningssignal.

För att inte EPROM och EEPROM-minnen skall skadas så är ordningen på aktiverings- och deaktiveringsoperationer väl definierade. I aktiveringen av kortet så ingår bl a följande:

- Mottag RST low
- Applicera VCC
- Sätt I/O i mottagar-läge
- Sätt VPP i inaktivt läge
- Applicera klocka

I deaktiveringen så ingår bl a:

- Mottag RST low
- Sätt klocka i passivt läge
- Sätt VPP i inaktivt läge
- Sätt I/O i passivt läge
- Inaktivera VCC

Programmeringsspänning, VPP

Programmeringsspänningen är en relativt hög spänning som används när något skall skrivas i icke-volatila minnen, dvs de minnen som behåller sin information även utan strömförsörjning. För att skriva till minne av typen EPROM behövs en utifrån pålagd spänning (12,5 eller 21 volt) medan EEPROM-minne kan skrivas med hjälp av en spänning som laddas upp i chipet. Av dessa minnestyper så är den senare långt mer populär eftersom den går att skriva över [se förklaring av minnestyper] och VPP blir därför allt mindre viktigt.

Klocksignal, CLK

Klockans signal synkroniserar de instruktioner som sker i mikroprocessorn. Ett smart kort kan innehålla en egen klocka men vanligtvis så får de en klocksignal utifrån via CLK. Klockfrekvensen är avgörande för hastigheten hos I/O-kommunikation. Enligt

³ *European Telecom Standard Institute*; har för övrigt tagit fram kraven till det smarta kortet till GSM-telefoner.

ISO finns två klockfrekvenser för smarta kort: 3,5795 MHz och 4,9152 MHz. En klockfrekvens på 4,9 MHz innebär alltså att 4,9 miljoner steg kan utföras per sekund, men det krävs många steg för varje instruktion. I Europa så är den lägre frekvensen den mest använda.

Data Input/output, I/O

Via denna anslutning så tar kortets mikroprocessor emot instruktioner samt utbyter data med omvärlden. ISO-standarden definierar en linje för utbyte av data mellan kort och omgivning och därför måste linjens ”riktning” ändras mellan mottagning och sändning. Detta tar en viss tid, *line turnaround time*, och måste hållas i åtanke av bland annat transmissions-protokollet.

Framtida bruk, RFU

De två sista kontaktblecken är inte bestämda av ISO utan är lämnade för framtida användning (Reserved for Future Use).

Smarta kortets minne

Det främsta syftet med smarta kort är att de ska vara en hållare av data som är lätt att ta med sig och att det går att läsa från det lika väl som att skriva till det. Kortets minne är alltså en central del i dess funktion. Det finns olika typer av minnen som fyller olika funktioner och här är några av dem:

Icke volatilt minne:

ROM, *Read Only Memory*, kallas även för programminne. Redan vid tillverkningen av chipet så skrivs programinstruktionerna i detta minne och de kan sen inte ändras. ROM är billigt men det går inte att ändra när det väl lämnat fabriken. En annan begränsning är att det tar ganska lång tid att tillverka dessa minnen, upp till några månader, och det måste beställas i stora kvantiteter för att bli billigt.

PROM, *Programmable read only memory*, minne som kan programmeras av användaren med hjälp av höga spänningar och möjligheten att skriva tas sen bort genom att säkringar bränns av.

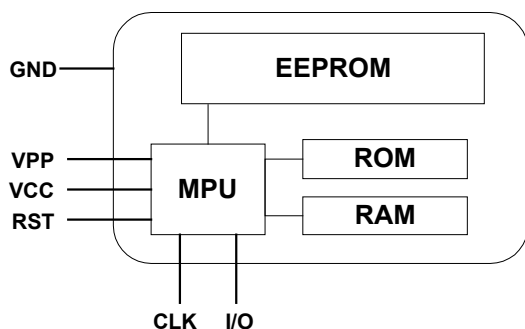
EPROM, *Erasable programmable ROM*, är per definition ett raderbart minne men EPROM raderas genom att det exponeras för ultraviolett ljus. Inneslutet i kortets mikromodul så kan dock inte uv-ljus komma åt EPROM-minnet och det är därför i praktiken inte raderbart när väl är inne i det smarta kortet.

EEPROM, *Electrically erasable PROM*, är minne som kan raderas elektroniskt. Det kan skrivas över mellan 10 000 och en miljon gånger och minnet kan bevara informationen utan strömförsörjning i upp till tio år. En annan fördel med EEPROM är att det kan delas upp i olika typer av minnen, t ex PROM eller ROM, genom att det flaggas i tillverkningen. EEPROM tar dock mer plats i mikromodulen än vad t ex EPROM tar.

Volatilt minne:

RAM, *Random access memory*, är ett så kallat arbetsminne. Det är volatilt och förlorar alltså sin information när strömmen bryts. När det är aktiverat så används det till att lagra resultat från beräkningar och I/O-operationer.

När det gäller de ovan nämnda minnestyperna så kräver de olika mycket utrymme samt kostar olika mycket. EEPROM är relativt dyrt minne.



Schematisk bild av ett mikroprocessor chips (MPU - Microprocessor unit). Bergdahl; *Smarta kort...*

CPU och Operativsystem

En av chipets centrala delar är CPU:n, (Central Processing Unit) alltså processorn. Det är processorn som gör att kortet verkligen kan kallas smart och den ger också många möjligheter till funktioner; inte minst när det gäller säkerheten. Det finns olika sorter av CPU och olika klockfrekvenser som används.

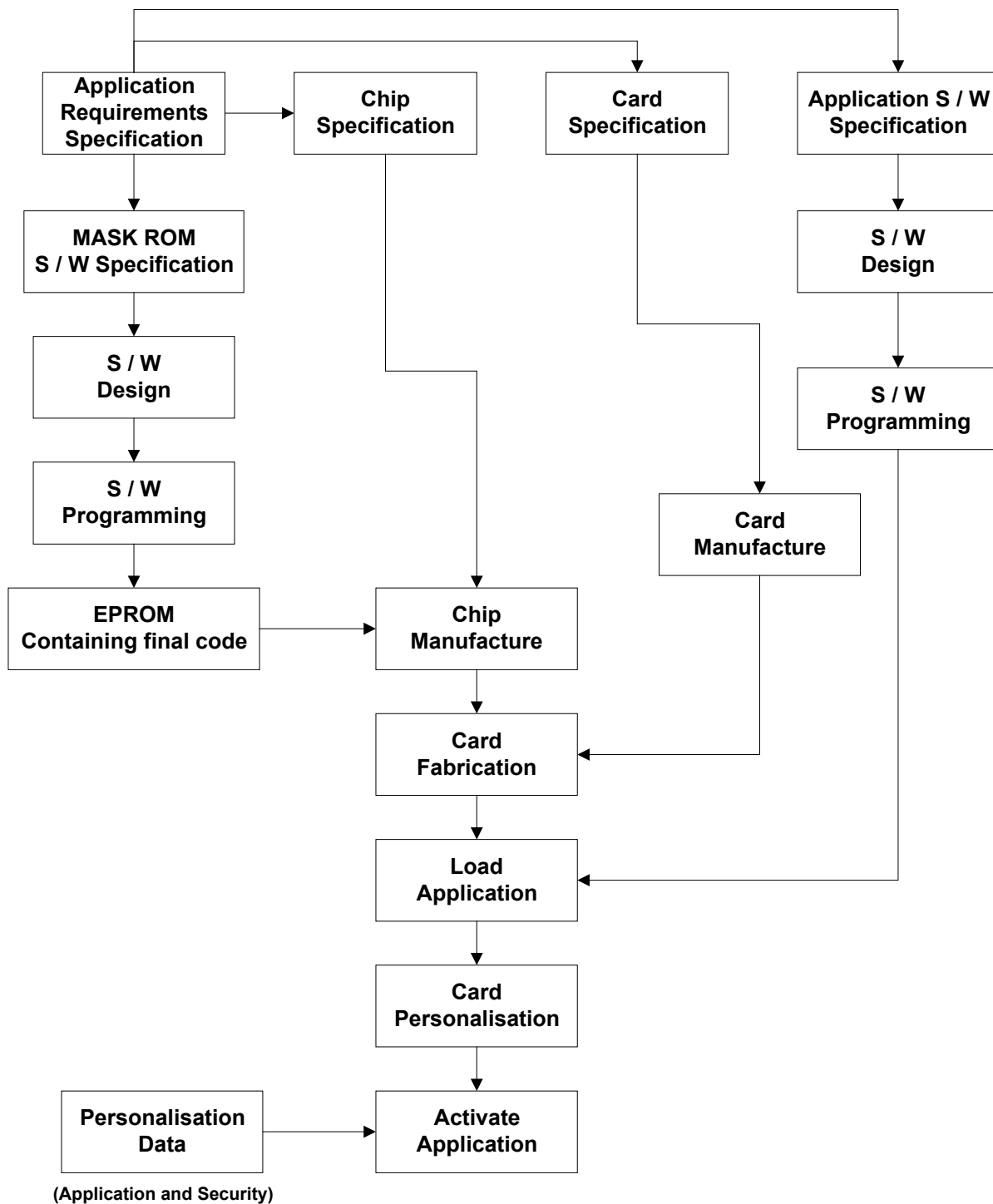
För att kortet skall fungera krävs att kortet har ett operativsystem. För smarta kort så kallas det *mask* och det bränns vid tillverkningen in i ROM-minnet. Olika korttillverkare använder dock inte samma operativsystem med kompatibilitetsproblem som följd. Det som i huvudsak är standardiserat är just återställningsproceduren som används som initiering varje gång kortet skall användas. Det svar som kortet då lämnar, Answer-To-Reset, är standardiserat enligt ISO 7816-3. Operativsystemet sköter hantering av datafiler men kan i vissa fall även handha exempelvis krypterings-algoritmer.

Tillverkning av ett smart kort.

När ett smart kort ska produceras så handlar det oftast om en relativt stor beställning som lämnas till tillverkaren. Kortet och chipet ska tillverkas och de skall fogas samman. Dessutom så sker vanligtvis viss programmering av chipet redan vid dess tillverkning. Vad gäller kortet så är följande specifikationer av intresse för tillverkaren; kortstorleken, kortets material, chipets placering, tryckegenskaper, eventuella magnet- och signaturremсор, eventuellt foto eller hologram etc. Chipets specifikationer bör täcka vilken mikroprocessor som ska användas, hur stor del av ROM som operativsystemet skall uppta, storleken på RAM, typ och storlek hos icke-volatila minnen, klockfrekvens, spänning- och strömstyrka, kommunikationsparametrar, återställningsrutiner etc.

Chipets programvara kan inkluderas på olika sätt. Det kan vara en del av mask i ROM men det är ganska omständligt för tillverkaren att vid produktionen lägga in denna programvara och det tar lång tid. Betydligt lättare är det om programvaran skrivs i

minne av typen PROM – då kan detta ske efter kortets tillverkning. Även kortets personifiering kan ske på detta sätt och sen bränner man bort säkringar så att det inte går att ändra det som skrivits i PROM.



Schematisk bild över tillverkningen av ett smart kort. Everrett; *Introduktion to Smart Cards*..

Dataöverföring

Överföring av information via en kanal som tillåter överföring i båda riktningar kan ske på olika sätt. *Half duplex transmission*⁴ kallas det när överföring bara kan ske i en riktning åt gången och om överföring kan ske i båda riktningar samtidigt så heter det *full duplex transmission*.

I den tidigare beskrivna standarden för smarta kort så finns bara definierat ett kontaktbleck för I/O och dataöverföring sker alltså enligt principen half duplex. Överföringen måste alltså byta riktning mellan det att kortet skall ta emot data och det att CAD ska ta emot data.

I huvudsak så finns det två kommunikationsprotokoll som används;

- T=0 half duplex character transmission
- T=1 half duplex block transmission

Säkerhet

Den stora fördelen med smarta kort är att transaktioner kan ske off-line. Detta ger snabbhet och enkelhet. Kortets mikroprocessor ser till att informationen som finns i kortet endast ges till mottagare som är behöriga. Det smarta kortet måste bevisa för CAD att det hör till systemet, man kallar det för igenkänning av kortet – *smart card authentication*. Motsvarande igenkänning av CAD kallas ofta *cross-authentication* och är nödvändig t ex för att CAD ska få uppdatera informationen på kortet. Det är alltså först när det smarta kortet och CAD ”känner igen varandra” som utbyte av hemlig information kan ske.

Det är av största vikt att det smarta kortet bevisar sin systemtillhörighet och att detta sker på ett säkert sätt. Det kan ske med hjälp av ett lösenord som kortet ger ut vid varje igenkänningsförsök. För att det skall vara effektivt, bör det ändras mellan varje användande.

Användaren måste ofta identifiera sig på något sätt. Ibland räcker det med att inneha kortet men vanligtvis så krävs någon annan form av identifiering t ex en pin-kod. Användaren slår in koden på CAD och den skickas sedan till kortet för att jämföras med en lagrad referens och om de överensstämmer så returnerar kortet en signal som ger klartecken för fortsatt kommunikation. Identifiering av användaren kan även ske genom biometriska metoder, exempelvis genom kontroll av fingeravtryck, iris eller rösten.

Kryptering

Kryptering är ett mycket effektivt sätt att bevisa kortets systemtillhörighet utan att avslöja hur det går till för omvärlden. Krypteringsnycklar måste distribueras i systemet så att meddelanden både kan krypteras och dekrypteras. Dessa nycklar måste genereras på något sätt och vanligtvis så sker detta med hjälp av olika former av algoritmer. DES, *Data Encryption Standard*, är en av de mest kända krypteringsalgoritmerna; framtagen av IBM i USA. Både kort och mottagare får ett slumpantal skickat till sig och den symmetriska algoritmen genererar två identiska nycklar som sen används för kryptering och dekryptering av information.

⁴ *The Architecture of Computer Hardware...* Irv Englander; sid 670

Asymmetriska algoritmer kan användas för att ytterligare öka säkerheten och då är krypteringsnyckeln inte den samma som dekrypteringsnyckeln. Det finns dock ett komplicerat matematiskt samband mellan nycklarna. Den mest kända asymmetriska algoritmen är RSA, döpt efter sina skapare *Rivest, Shamir* och *Adleman*, och den bygger på svårigheten att dela upp stora primtal i faktorer.

Symmetriska algoritmer

DES-algoritmen är vanligt förekommande i smarta kort. I varje smart kort och CAD finns en hemlig krypteringsnyckel, vanligtvis 64 bits långa. För att korta beräkningstiderna kan en så kallad accelerator byggas in i kortet. Systemet tar fram unika nycklar åt varje kort, differentierade nycklar, som ofta är en kombination av huvudnyckeln och t ex kortets serienummer. Differentierade nycklar gör att även om ett korts nyckel avslöjas så avslöjas ändå inte systemets huvudnyckel och det räcker med att ta det aktuella kortet ur bruk. Nackdelen är att om huvudnyckeln, som finns lagrad i varje CAD, avslöjas så måste alla kort i systemet få nya differentierade nycklar och det är naturligtvis omständligt och kostsamt. Av den anledningen finns det CAD med en intern kortläsare och då kan ett smart kort användas för att lagra nödvändiga DES-nycklar. De interna DES-korten kallas för SAM, *Security Application Module*, och kan lagra även andra hemliga data.

Asymmetriska algoritmer

Asymmetriska algoritmer bygger på principen att det är olika nycklar i kort och CAD men att ett samband utnyttjas för igenkänning. Normalt så används en så kallad *trapdoor*, CAD använder en känd nyckel för att verifiera en från kortet utsänd signatur som innehåller dess hemliga nyckel. Ovan nämnda algoritm RSA används flitigt men den kräver att kortet har en co-processor som minskar beräkningstiderna.

Transaktionsnycklar

När det smarta kortet och CAD "känt igen varandra" så kan en hemlig men temporär nyckel användas. Detta för att om koden under den fortsatta kommunikationen blir avlyssnad, inte skall avslöja den riktiga nyckeln.

Krypteringsalgoritmer skrivs vanligen in i kortets operativsystem och lagras i ROM redan vid kortets tillverkning.

Rent hårdvarumässigt så kan kortet förses med olika detaljer för att öka säkerheten. En slumpgenerator som underlättar kryptering kan vara inbyggd, detektorer som avslöjar missförhållanden vad gäller temperatur, klockfrekvens, ljus och VCC kan också vara en del av hårdvaran. Strömförvrängning är en annan metod för att öka säkerheten och då kamouflerar man den egentliga strömstyrkan så det inte skall gå att dra slutsatser om de data som skickas.

Teknik hos Cashcard

När det gäller tekniken hos de cashcard som används i Sverige så är det svårt att få fram exakt information eftersom den ofta är hemlig. Korten använder samma teknik som ovan är beskrivet för smarta kort men de exakta specifikationerna finns inte offentliga.

EEPROM-minne är självklart i dagens moderna kort och man arbetar hela tiden för att få plats med mer minne på samma yta.

CashLoad Device

Detta avsnitt avhandlar systemet för laddning av cashcardet lite mer utförligt än tidigare. Här beskrivs hur laddaren ser ut och vad den består av. En beskrivning av dess hårdvaru- och mjukvarudelar ges samt en översikt av dess funktioner. Avslutningsvis ges en schematisk bild av hur själva överföringssystemet fungerar mellan kort, laddningsenheten och banken.

Eftersom vi i våran studie haft mycket kontakt med ICL Financial Systems, som är ett företag som finns i Linköping och som tillverkar laddningsenheter så kommer detta avsnitt att beskriva hur deras laddningsenheter är uppbyggda.

ICL har olika typer av laddningsterminaler som heter PaySec 201/205 och PaySec 90x. Dessa terminaler fyller samma funktioner och liknar varandra förutom att den förstnämnda är avsedd för inomhusbruk emedan PS 90x är för utomhusbruk.

Hårdvara

Hårdvaran i terminalerna utgörs av följande typer av enheter. Vad som ingår i respektive terminal preciseras inte.

- Terminal med ett processorkort.
- Minne för lagring av program utgörs av ett 512 kb PROM (se avsnittet om kortet fördetaljer) samt olika typer av RAM-minnen.
- Klocka för realtid. Terminalen har en batteri back-up och klockan håller tid och datum i terminalen om strömtillförseln skulle brytas. Klockan åtkomlig för vissa inställningar såsom aktuell tid och datum samt start och stopp tid.
- Tangentbord med siffror och 10 funktionstangenter.
- 2*16 tecken LCD display med ljusfunktion.
- IC-kort läsare. Denna läsare är kompatibel med ISO 7816 standarden och klarar både T=0 och T=1 protokoll. Läsaren är en kontaktläsare, d.v.s. att kortet måste komma i kontakt med läsaren för att överföring skall kunna genomföras.
- SAM-kort (Secure Application Module). Detta kort döljer säkerhetsinformationen i systemet.

Varje terminal har två olika kommunikationsanslutningar:

- LAN-port. Det interna LAN kan ha upp till 32 adresser. Överföringshastigheten ligger på 9600 bps
- 2 RS-portar. Ett externt modem kan kopplas till en av portarna för kommunikation med bankernas databas.

Mjukvara

Operativsystemet och drivrutinerna för hårdvarorna i laddningsterminalen kallas för EFTOS och är skrivet i assembler och är fullständigt för att lösa kopplingen mellan hård och mjukvara. Nästa lager som utgör interface till själva applikationen kallas för API

(Application Programming Interface) och är skriven i ett språk som ASM-51 och C-51. Applikationen de olika laddnings processerna är skriven i C.

Terminalen arbetar i sex olika funktioner:

- Laddning av mjukvara, kan ske från en vanlig PC eller via telefon kommunikationen.
- Uppstart. Vid uppstart känner terminalen av om det finns ett SAM-kort anslutet och om så är bekräftar terminalen kortet. Vid uppstarten sker även en kontroll av om det finns några kalla meddelanden liggandes i minnet (eng. Cold messages), vad detta är kommer att framgå senare i avsnittet om själva överföringen.
- Installation. Sker när ett nytt SAM-kort installerats eller via startup proceduren om man så anger. Detta kommer inte att avhandlas vidare.
- Ledighetsfunktion (eng. Idle). Den fas då terminalen väntar på uppgifter såsom insättning av kort, tangenttryckning, försök att sända kalla meddelanden.
- Laddningsfunktionen. När kort satts i läsaren och laddning har angivits från tangentbordet så körs själva laddningsprocessen igång, vilket förhoppningsvis resulterar i att kortinnehavaren får lite mer elektroniska pengar på fickan att konsumera.
- Saldofunktionen. När detta anges av kortinnehavaren så kommer aktuellt saldo för kortet att visas under tre sekunder.

Systemsäkerhet

Som tidigare nämnts så är det i SAM-kortet som informationssäkerheten sitter. Här sker en form av kryptering och s.k. MAC-beräkningar (Message Authentication Code) och verifiering, vilket är sätt att kontrollera äkthet i informationen och den pågående överföringen. SAM-kortet är en central del i systemet, vilket lätt inses, och intressant i många avseenden. Av sekretsskäl kommer dock inte SAM-kortet och lösningen av säkerhetsaspekterna att behandlas mer ingående än så här.

Ytterligare en del i säkerheten tillkommer i och med proceduren med PIN-kod som genomförs innan laddning av Cash-kortet sker.

Informationsöverföring

Följande avsnitt avser att precisera händelseförloppet vid ett laddningstillfälle.

När kort-innehavaren placerat kortet i IC-kortläsaren och valt laddafunktionen kommer kontakt att upprättas mellan kortet och det bankkonto som tillhör kort-innehavaren för överföring. Det finns dock en del enheter där emellan. Terminalen kommer via ett externt modem att ringa upp en modempool som i sin tur är ansluten till en värd (Frontend) för de, i systemet ingående, banker. Det är i värddatabasen som validitetskontrollen sker, via kontroll med den, för tillfället, aktuella banken. Till värdbasen finns det back-up system anslutna för att möjliggöra spårning och upprättande av förlorad information, allt för att öka säkerheten i systemet. Via värdbasen är det möjligt att gå in och spåra varje enskild transaktion, vidare så är det möjligt att, i den andra ändan av systemet, följa hur de överförda pengarna konsumeras runt om i landet.

Format

För överföringen mellan värden och terminalen finns fyra (åtta) olika meddelande format.

- **C/R-Par** (PARametrisation)
- **C/R-PUR** (PURse inquiry)
- **C/R-TRA** (TRAnsaction confirmation)
- **C/R-STC** (Status Card incident)

C/R-Par sänds i installationsfasen när första kontakten mellan terminal och värden inleds. Detta för att terminalen ska hämta in parametrar från värden. C-PAR (uppropet) innehåller uppgifter som t.ex. terminal-ID, mjukvaruversion och nyckel-ID. R-PAR (Svaret) kommer från värden och innehåller bl.a. datum och tid och information till SAM-kortet för MAC.

C /R-PUR sänds då överföringen skall initieras. C-PUR innehåller t.ex. informatin som specificerar kort-innehavaren, konto, summa samt SAM och nyckel information. R-PUR svarar med en mängd information där saldo och övriga uppdateringar av kontohavaren är ett par exempel.

C/R-TRA sänds som bekräftelse på att överföringen är genomförd.

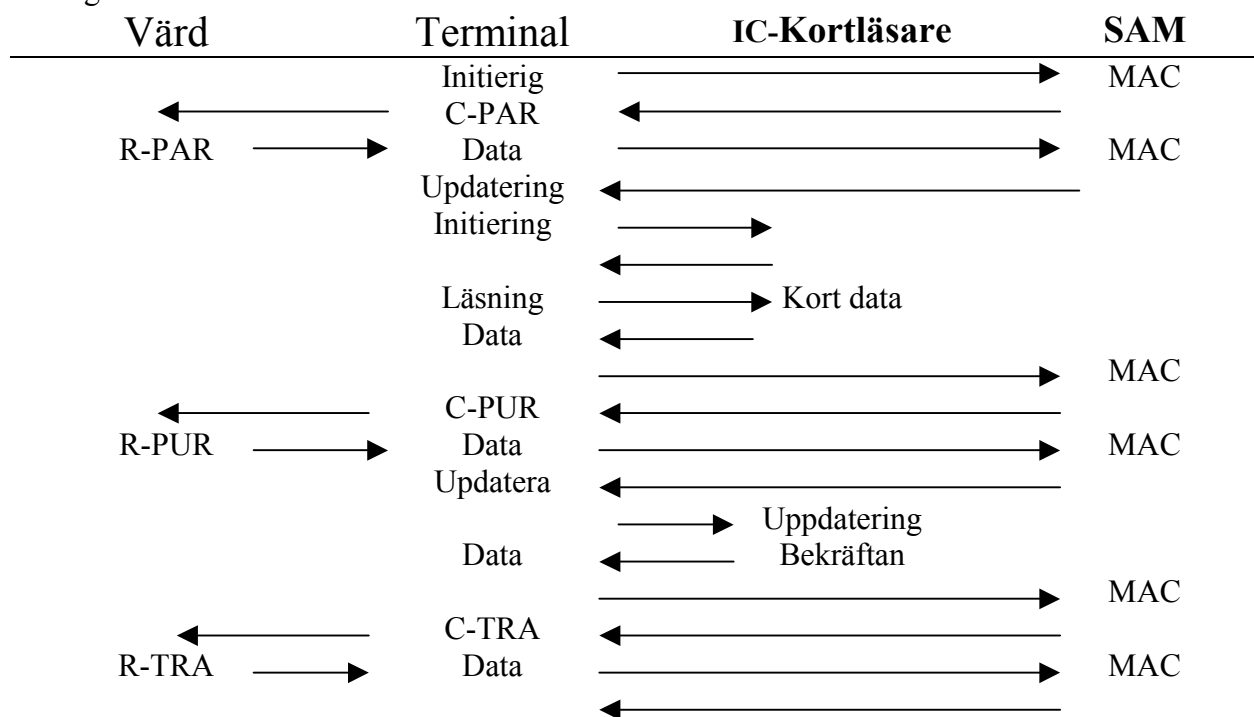
C/R-STC sänds mellan terminalen och värden om det står avbrott eller annat fel i systemet.

Hela flödet bygger på upprop- och svarsformat där det är terminalen som initierar kommunikationen på kommando från kort-innehavaren. Nedan görs ett försök till att skapa en enkel och schematisk bild över informationsflödet.

Informationsflödet

Hela processen startar med att terminalen erhåller en begäran från användaren att ladda kortet. Terminalen börjar med att kontrollera statusen på SAM-kortet. En C-PAR sänds iväg till värden och en R-PAR erhålls som svar och data går vidare till SAM för utförande av MAC beräkningar. Terminalen uppdateras och startar IC-kortläsaren och väntar på användarens instruktioner om vilket belopp som önskas (eller önskan om saldo) och en bekräftelse. Kortläsaren skickar en signal till terminalen när den känner av kortet i laddaren och terminalen skickar en begäran till processorn på kortläsaren att läsa in data från kortet. Datat sänds till terminalen och en ram för förfrågan skapas och sänds, via SAM för påfyllning av säkerhetsinformation, till värden som en C-PUR och ett R-PUR kommer tillbaka efter behandling till SAM-kortet för kontroll och därefter sker uppdatering av kortet via läsaren. När läsaren bekräftar att uppdateringen är slutförd skapas en transaktionsbekräftelse ram som fylls med information från SAM-kortet och en C-TRA och besvaras med en R-TRA från värden och en slutlig kontroll sker i SAM-kortet. Så långt är allt gott och denna process kan utläsas i figuren nedan.

Fig.



Om det uppstår fel någonstans under resans gång så vidtas vissa åtgärder. Först så skapas en incident format ram i terminalen som fylls med fel information och, via SAM som vanligt, sänds till värden som kvitterar och terminalen kontrollerar svarets äkthet och innehåll. Dessa meddelanden sänds vid de tillfällen det uppstår fördröjningar i systemet som kan tolkas som kommunikationsfel. Här kommer det tidigare nämnda begreppet om kalla meddelanden in i bilden. Om överförings-avbrottet inträffar under ett C-PUR meddelande så kommer ett C-STC att skickas. Om däremot ett avbrott inträffar under ett C-STC eller C_TRA meddelande så sparas meddelandet, det blir liggande och ”kallt”, och en process för återsändande av kalla meddelanden startar. Terminalen kommer att spärras för ytterligare användande tills det att kontakten återupprättats och de kalla meddelandena har kommit fram och slutförts. Om avbrott inträffar under ett C-PAR startar även denna process men terminalen låses inte utan nya försök kan påbörjas.

Så fort återsändningen av ett kallt meddelande har påbörjats så kommer terminalen att be användaren att återta sitt kort. I terminalen startar en timer vars värdesatts vid transaktionens början i R-PAR. Terminalen kommer att försöka återsända meddelandet när timern har räknat ner. Om ingen kvittens erhålls multipliceras timertiden *2 och startar om och återsänder igen när den räknat ner o.s.v. utan övre gräns för hur många återsändningar som kan ske. Däremot finns en övre gräns för hur lång tid som kan gå emellan återsändningarna. När maxvärdet nåtts så förblir tiden emellan konstant. Detta pågår tills kontakt återupprättats och alla kalla meddelanden har retts ut. Medan tiden tickar kan man sätta in ett nytt kort i läsaren för att ladda. Då kommer nedräkningen att brytas och en återsändning sker direkt. Vid lyckat resultat försätter terminalen som vanligt annars så låses terminalen och timern går återigen igång.

Som tidigare nämnts så skapas ramar för de olika meddelandena. Dessa är av enkel sort och består ett start och ett slut block med data blocket mitt emellan. Data blocken är 252

bytes stora. Slutblocken skiljer sig i de fall att data överföringen måste ske i flera block så att värden vet om det kommer eller inte. Värden bekräftar i så att den är beredd på att ta emot ytterligare data. Om fel uppstår så att värden inte uppfattar att det kommer mer data utan bekräftar en slutförd överföring sker högst tre återförsök av terminalen därefter skapas felmeddelande. Värden bryter normalt kontakten om ingen överföring sker inom 30 sekunder. För att förhindra detta sänder terminalen ut ett s.k. dummymessage var 20:e sekund under pågående transaktioner.

Avslutning

En av de mest avgörande aspekterna för cashcard-systemet och smarta kort över huvud taget är säkerheten. När ett system idag sägs vara säkert så kan det vara hela sanningen men precis som säkerheten hela tiden utvecklas så utvecklas också teknikerna för att ta sig förbi spärrarna. Särskilt smarta kort som fungerar som betalmedel utsätts för stora prov eftersom det lockar många med kriminella uppsåt. Drömmen om att bräcka systemet och skapa sig själv en sedelpress gör att kortutvecklarna aldrig kan slå sig till ro och lita på att systemet är säkert. För att cashcard-systemet ska få opinionen med sig så är det självklart också av största vikt att säkerheten garanteras med god marginal.

Om cashcard-systemet skall få en ordentlig genomslagskraft så måste dess nytta verkligen belysas för konsumenterna, inte bara för bankerna. Dessutom så måste systemet göras lättillgängligt för gemene man; kanske bör man vänta med de mer avancerade tekniska finesserna och se till att korten kommer i bruk t ex som betalmedel i automater etc. När folk väl blivit bekanta och vana vid betalkorten så kommer automatiskt en efterfrågan efter att kunna ladda upp dem med större summor, att kunna använda dem i fler sammanhang, att bygga in flera funktioner i ett och samma kort osv. En förutsättning för att cashcard-systemet skall vinna önskad genomslagskraft i Sverige är just att man lyckas nå de vanliga konsumenterna och övertyga dem om kortens nytta. Då Sverige dessutom är ett teknikvänligt land med människor som inte är alltför konservativa så är chanserna goda för att satsningen blir lyckad.

Referenser

Muntliga referenser

ICL FINANCIAL SYSTEMS AB

Ulf Nilsson, Specialist Consultant Customer Interaction

ICL

Patrik Jansson, System Engineer

ICL FINANCIAL TERMINALS AB

Nils-Göran Albinsson, Systems Manager

Ulf Andersson, Systems Security Manager

ICL / ICL FINANCIAL TERMINALS AB

Teknikringen 8
P.O. Box 1938
581 18 Linköping

ICL FINANCIAL SYSTEMS AB

Torshamnsgatan 36
P.O. Box 40
164 93 Kista

Litteraturreferenser

Irv Englander; *The Architecture of Computer Hardware and Systems Software*. Wiley & Sons, Inc. 1996.

Dr David B Everett; *Smart Card Technology*.

Artikel på adressen: <http://www.smartcard.co.uk>.

Thomas Bergdahl; *Utlandsrapport från Sveriges Tekniska Attacher – Smarta Kort, Teknik och tillämpningar i USA*. 1995

Teknisk Specifikation; *ICL CashLoadDevice Specification*; internt dokument från ICL, Linköping

Allmän information:

<http://www.sebank.se/sebank/kort/cash.html>