INFORMASJON OM KORTSYSTEMET

Innholdsfortegnelse (overordnet):

Sikkerhet
Kort
Bruk av kort
Avtaler
Minibank
EFTPOS
Vanlige spørsmål om kortbruk og sikkerhet

Banker i Norge har et samordnet kortsystem.

Dette innebærer at alle kort som er utstedt av bank og som omfattes av det felles regelverk, kan benyttes i alle betalingsterminaler og / eller kontantautomater som inngår i samordningen. Regelverket finnes i de to bankforeningers samling av avtaler og regler. Se Avtale- og regelverksamling for innenlands betalingsformidling på www.fnh.no; Publikasjoner. Regelverket kan bestilles fra FNH.

Alle disse kortene skal ha "bank axept"-logoen. Alle minibanker og alle brukersteder skal være merket med "bank axept". <tegnet eller innskannet bilde>

En del av de vanlige spørsmål om kortbruk finner du et annet sted på denne siden:

Disse sidene omfatter det norske nasjonale kortsystemet.

Mange av kortene som er utstedt av norske banker, har en internasjonal tilknytning. For å få mer informasjon om internasjonal bruk, kontakt din bank.

-

SIKKERHET

Innenlands bruk av "bank axept"-kort er basert på kombinasjonen av magnetstripe og PIN.

Formålet med dette er å oppnå identifikasjon av kort og kunde.

PIN

PIN (Personlig Identifikasjons Nummer) er en firesifret kode. For allmene regler for oppbevaring og bruk av PIN, se her :

Norske banker følger standard ISO 9564 for behandling av PIN.

Det er ikke mulig å finne et korts PIN-kode ut av innholdet i magnetstripen.

Generering av PIN

Den enkelte kontobank er ansvarlig for generering (produksjon) av PIN.

Bankenes Standardiseringskontor (BSK) har hjemmel til å stille krav til bankenes generering av PIN. BSK kan inspisere bankenes lokaler og rutiner.

Kortholders bruk av PIN

PIN er en hemmelig personlig kode. PIN brukes på kontantautomater og terminaler på brukersteder i stedet for håndskrevet signatur.

Kortholder bør straks lære seg PIN-koden utenat og makulere brevet fra banken der PIN er skrevet ned. Kortholder bør lese nøye kontrakten om kortbruk som er inngått mellom kortholder og bank.

Kortholder må aldri oppgi PIN-koden til andre, ikke en gang til personer som utgir seg for å være fra banken eller fra politiet og andre myndigheter.

Bankene vil gi kortholdere nærmere informasjon om oppbevaring av kort og kode samt råd om hvilke koder som ikke bør velges ved eventuelt skifte av kode.

Kortholder må f. eks. ikke skrive koden på kortet eller på en papirlapp som oppbevares i samme lommebok eller kamuflere PIN-koden i et fiktivt telefonnummer.

PIN-koden skal ikke brukes under slike forhold at andre lett kan se den. Uansett anbefales det at når man taster PIN, bør man forsøke å plassere hendene og kroppen slik at det blir enda vanskeligere for uvedkommende å se hva som tastes.

Verifikasjon av PIN

Prinsippene for PIN-verifikasjon er de samme både for spor 2 og spor 3 kort.

Når en kortholder har tastet inn en PIN-kode på en minibank eller et brukersted, skjer følgende:

- Den inntastede PIN krypteres (dvs. gjøres ugjenkjennelig for uvedkommende og dermed umulig å avlytte) og sendes til bankmiljø.
- I bankmiljø vil den krypterte PIN bli dekryptert inni et godkjent sikkerhetssystem.
- Inntastet PIN vil gå inn i en beregning som illustrert:

Kryptografiske kontroller

Det er obligatorisk å kontrollere PIN ved bruk av "bank axept"-kort.

Regler for håndtering av feil PIN finnes under kortkontrollene.

Alle kort har en sikkerhetsverdi i magnetstripen som skal kontrolleres for å verifisere at kortet er ekte. Denne verdien har forskjellig navn (CVV, CVC eller CSN) avhengig av kortutsteders system.

For spor 3 kort kan i tillegg sikkerhetsverdien CSN kontrolleres for å verifisere at kortet ikke er urettmessig blitt endret.

-

SIKKERHET I SYSTEMENE

Alle forespørsler og meldinger i kortsystemet er beskyttet mot at uvedkommende kan endre, slette eller sette inn data.

PIN-data er plassert i en PIN-blokk som er laget i samsvar med standarden ISO 9564 og så er kryptert for å beskytte mot innsyn.

Krypteringsnøklene som brukes til beskyttelsen av PIN, ligger i en såkalt krypterende PIN-pad. Dette er en enhet med innebygget tastatur som sørger for at inntastet PIN umiddelbart går rett inn i et fysisk og logisk sikkert miljø. Alle minibanker og betalingsterminaler må ha en krypterende PIN-pad for å bli godkjent til bruk i det norske kortsystemet. BSK kan godkjenne terminaler til bruk i kortsystemet. For å bli godkjent må den fysiske og logiske sikkerhet rundt den krypterende PIN-pad først ha blitt evaluert av et internasjonalt anerkjent laboratorium.

BSK forvalter reglene for godkjennelse av minibanker og betalingsterminaler. BSK kan distribuere

disse til mulige terminalleverandører.

Krypterende PIN-pads må ha en høy grad av "tamper resistance", dvs. at de skal kunne motstå angrep eller forsøk på modifikasjon.

Prinsippet med at en nøkkel skal brukes til ett og bare ett formål, er gjennomført. Det brukes separate nøkler til å verifisere PIN og til å kryptere data som overføres.

Nøkler for verifikasjon av PIN finnes ikke ute i minibankene eller betalingsterminalene. Disse nøklene eksisterer bare i sikrede miljøer i bankenes sentrale systemer.

KORT

Norske bankkort er magnetstripekort, basert på internasjonale standarder. På denne siden skiller vi mellom det fysiske kortet og representasjonen av informasjon i magnetstripen.

Betalingskort må behandles som en verdigjenstand.

Magnetstripen kan bli fysisk skadet og ubrukelig hvis den utsettes for påkjenninger. For å beskytte kortene minner vi om at:

- Kortet må ikke utsettes for magnetiske eller elektromagnetiske felter da dette kan slette eller ødelegge innholdet i det. Derfor bør ikke kortet lagres oppå høyttalere eller helt inntil PC-skjermen. En annen alminnelig kilde til avmagnetisering er magnetlåsene som finnes på enkelte typer håndvesker.
- Kortet må ikke utsettes for sterk varme eller direkte sollys.
- Kortet må ikke brettes eller tilsmusses.

Klikk her for å se hvilke standarder som brukes for det fysiske kortet.

Klikk her for å se teknisk informasjon om magnetstripen.

BANKKORT SOM FYSISK LEGITIMASJONSDOKUMENT

Ditt bankutstedte kort kan også inneholde et legitimasjonsdokument (Bankkort med bilde).

De to bankforeninger har vedtatt regler for utforming av bankkort som legitimasjonsbevis. Når ett og samme fysiske kort brukes både som "bank axept"-kort og som legitimasjon, skal legitimasjonen plasseres på baksiden. Legitimasjon skal ha følgende informasjon:

Kundens navn,

Legitimasjonskortets utløpsdato,

Kundens fødselsnr,
Kundens kontonr,
Kontrollnummer.

Legitimasjonen skal være utstyrt med bilde av kortholder.

Legitimasjonen skal ha et signaturpanel som viser kortholders underskrift.

Regelverket for bankkort som legitimasjon forvaltes av Bankenes Standardiseringskontor.

Bankkortet skal være legitimasjon ved bruk av sjekk. Mottaker av sjekken skal kontrollere bilde og underskrift på bankkortet og verifisere at bankkortets og sjekkens kontonummer stemmer overens. Bankkortets kontrollnummer skal skrives på baksiden av sjekken.

BRUK AV KORT

Klikk her for å se hvilke kontroller som gjøres ved bruk av kort i minibank eller ved varekjøp på terminal.

AVTALER

Alle kortbrukere har inngått en avtale med sin bank.

Avtalen inneholder beløpsgrenser for kortholders ansvar. Som en generell regel kan det sies at kortholders økonomiske ansvar er lavest (500 kr) når kortholder har behandlet kort og kode med aktsomhet og dersom kortholder melder fra umiddelbart når det er mistanke om at kortet, med eller uten kode, er kommet bort. Dette vil bli endret i forbindelse med den nye avtaleloven – da vil beløpet være kr. 800.-. Ved grov uaktsomhet eller misbruk med forsett gjelder andre beløpsgrenser. For å se hvilke beløpsgrenser som gjelder for den enkelte kortholder, henvises det til kortholders avtale med banken.

Ved tvister om hvilken beløpsgrense som kommer til anvendelse i en sak hvor kort er blitt misbrukt, kan kortholder bringe saken inn for Bankklagenmenda. Kontobank er pliktig til å gjøre kunden kjent med mulighetene for å få saken inn til behandling i Bankklagenemnda.

Mønsteravtalene vil undergå revisjon når den nye Finansavtalelov gjøres gjeldende i juli 2000.

Innholdet i den nye Finansavtaleloven er på dette punkt svært forskjellig fra dagens regler. Foruten den generelle endringen av kortholders ansvarsgrense til 800 kr innfører loven en grense for kortholders ansvar på maks 8000.- ved grov uaktsomhet. Dersom kortholder har misbrukt kortet forsettelig, gjelder ingen grense for hans / hennes ansvar.

MINIBANK

Uttrykkene minibank og kontantautomat brukes som synonymer. Det kan også være nyttig å kjenne den engelske betegnelsen ATM (Automated Teller Machine).

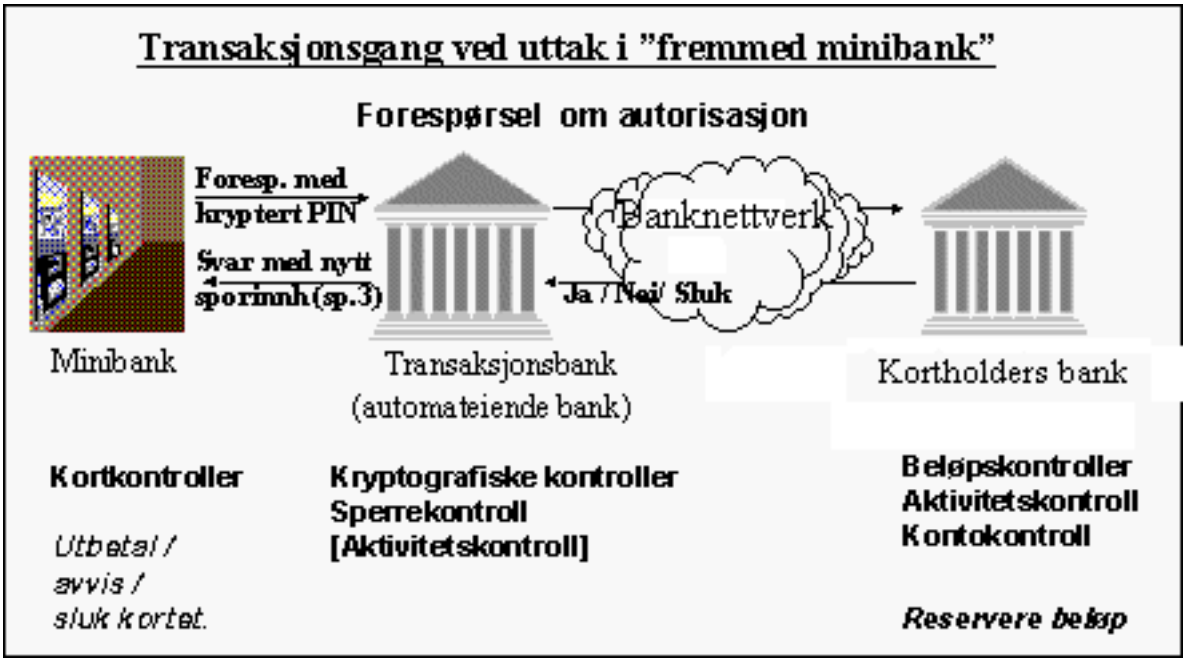
Uttak av kontanter i norske kroner eller fremmed valuta der dette tilbys, er en tjeneste til alle kort merket med "bank axept". Enkelte minibanker kan også tilby andre tjenester. Dette er ikke samordnede tjenester slik at de ikke nødvendigvis er åpne for kortholdere i andre banker enn automatens eier.

De første minibankene ble tilgjengelige for publikum i Norge i 1978-79. Ved utgangen av 1998 var det 1944 minibanker i Norge. (kilde: Norges Bank). Antallet har vært langsomt stigende de siste fem årene. I 1998 ble det gjort 103 millioner kontantuttak i minibank. Også dette tallet har vært langsomt stigende.

De fleste minibanker finnes i tilknytning til banker, enten som lobbyautomater inne i banklokalet eller med tilgang utenfra.

Minibankene skal skrive nytt sporinnhold i de kortene som bruker spor 3. Feltene som beskriver aktivitetsdata vil bli skrevet i kortet etter hvert uttak.

Skjematisk fremstilling av uttak i minibank:



Uttak i minibank fører til at beløpet umiddelbart reserveres på kortholders konto.

Selve transaksjonen til belastning av kortholder blir generert senere. Denne går via en

avregningssentral som sørger for at det automateiende bank blir kreditert det beløp som er tatt ut, fra kortholders bank.

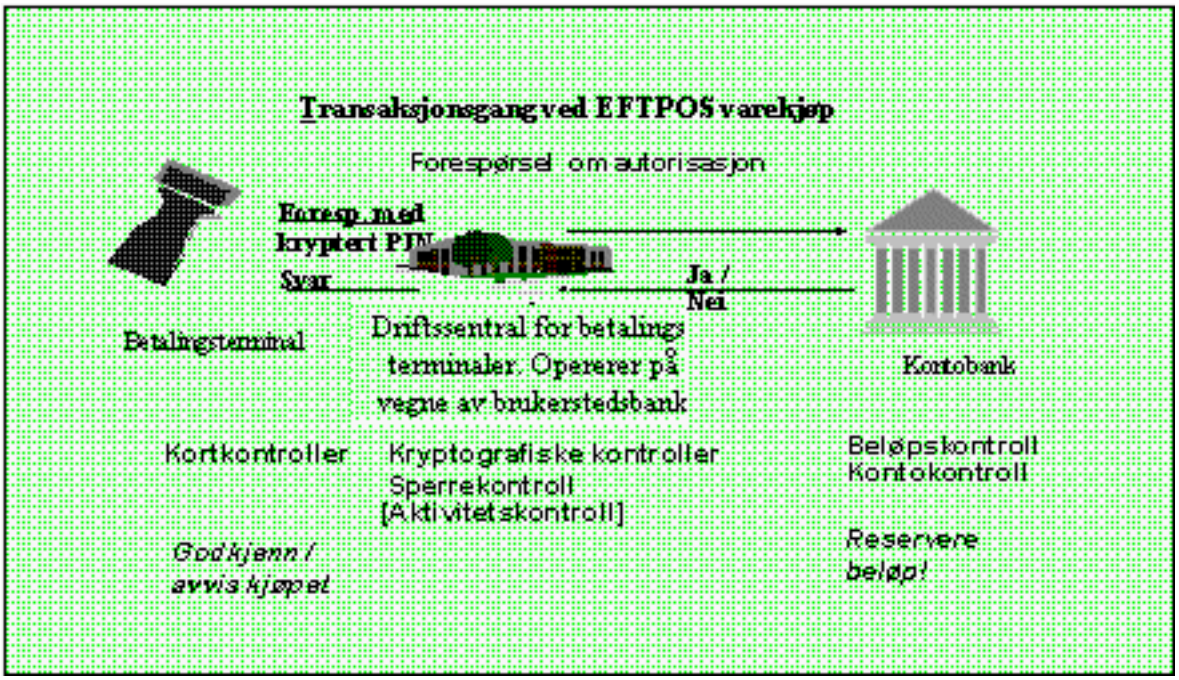
BETALINGSTERMINALER (EFTPOS)

Ved EFTPOS forstås vanligvis bruk av betalingsterminaler ved kjøp av varer og tjenester. EFTPOS står for Electronic Funds Transfer at Point of Sale.

Betalingsterminaler på brukersteder vil være knyttet mot en driftssentral. Driftssentralen vil ha avtale med brukerstedets bankforbindelse (transaksjonsbank) om å autorisere og samle inn transaksjoner.

Ved utgangen av 1998 var det 52235 betalingsterminaler i Norge på over 38000 brukersteder. (kilde Norges Bank). Antallet har steget hurtig og er nesten fordoblet i løpet av de siste fire årene. I 1998 ble det gjort: 230 millioner varekjøp med bankkort. Hvert av de siste årene har antallet varekjøp økt med 25 - 30 prosent i forhold til året før.

Skjematisk fremstilling av EFTPOS varekjøp:



EFTPOS varekjøp fører til at beløpet umiddelbart reserveres på kortholders konto.

Driftssentralen foretar avstemming av brukerstedene.

Selve transaksjonen til belastning av kortholder blir generert senere. Denne går via en avregningssentral som sørger for at det blir generert kredittransaksjoner til brukerstedet.

Reserveløsning

Selv om det norske kortsystemet er et on-line system, vil det fra tid til annen hende at det ikke oppnås kontakt mellom terminal på brukersted og bank / datasentral som mottar transaksjoner.

Ved teknisk svikt tillates det at brukersteder med betjente terminaler benytter en reserveløsning. I reserveløsningen må kortholder legitimere seg og signere på en papirslipp der kontonummer og transaksjonsbeløp er fylt ut. Brukerstedet er forpliktet til å sjekke kortholders legitimasjon.

Reserveløsning kan ikke benyttes for beløp over 1500 kr. ved elektronisk reserveløsning. For andre typer reserveløsninger er grensen 2500 kr.

Transaksjonsbank skal snarest mulig og senest innen fem virkedager etter at reserveløsningen er benyttet på brukerstedet, overføre transaksjoner dannet på grunnlag av reserveløsningen, til kontobank.

ELEKTRONISK HANDEL

Det finnes pr. i dag ikke noe felles norsk kortmerke for elektronisk handel over Internett på samme måte som "bank axept"-merket brukes på butikker og salgssteder.

Det norske kontonummeret skal derfor ikke brukes for belastning på Internett ved kjøp av varer eller informasjon.

De internasjonale kortselskapene har løsninger for handel over Internett.

NETTBANK

De fleste norske banker har en nettbanktjeneste i drift for f. eks. regningsbetaling og overføring mellom egne konti. Den enkelte bank er selv ansvarlig for sikkerheten av denne og for sikkerheten mellom bankkunde og egen kontobank. Telefonbanker og internettbanker er ikke en samordnet tjeneste og omtales ikke derfor på disse sidene.

VANLIGE SPØRSMÅL OM KORTBRUK OG SIKKERHET

1. *Hva skal jeg gjøre hvis jeg mister kortet mitt, eller om det blir stjålet?*

   a Da må du straks melde fra til din bank.

   a I bankenes åpningstid er det kortholders egen bank som skal varsles. Noen banker har også opprettet egne nummer for 24 timers assistanse.

   a Når banken du er kunde i, ikke er åpen, kan alle norske bankkunder ringe **Bankenes Meldingstjeneste, tlf 800 30 250**. Betjeningen på meldingstjenesten kan i dag blokkere samtlige bankutstedte norske korttyper, med noen få unntak.

2. *Garanterer bankene at kunden ikke lider noe tap fra det tidspunkt et kort er meldt stjålet?*

   Standardkontrakten mellom bank og kortholder opererer med en egenandel på 500 kr. Denne vil bli endret til 800 kr. f.o.m. 1.7.2000. Utover det risikerer kunden ingenting dersom han / hun opptrer normalt aktsomt. Her er det svært viktig at kunden lærer seg koden utenat, og at denne ikke nedtegnes noe sted. Koden skal i alle henseende holdes hemmelig. Kortet må betraktes som et verdidokument og behandles deretter.

3. *Hva er "grov uaktsomhet" i denne sammenhengen?*

   Det beste eksemplet på grov uaktsomhet er å skrive koden på kortet eller på annen måte oppbevare kort og kode på samme sted. Det må også understrekes at koden er en personlig hemmelighet og skal ikke fortelles til andre, ikke en gang til banken eller til politiet. Hvis kunden har opptrådt grovt uaktsomt har forsettelig bidratt til misbruk, eller har unnlatt å melde fra til banken om tap av kort, kan kunden bli ansvarlig for høyere beløp enn egenandelen. For eksakte beløpsgrenser henvises til avtalteksten i kundens kontrakt med banken, jfr. også de nye reglene i den nye Finansavtaleloven.

4. *Kan bankene innestå for at bankkort er 100% sikkert?*

   Hvis kort og kode brukes i samsvar med den kontrakten som er inngått mellom bank og

kortholder, kan kunden være trygg på at bankkortet ikke vil påføre ham økonomisk tap utover standard egenandel.

5. *Hva bør jeg gjøre hvis jeg tror at noen har fått tak i PIN-koden min?*

   Da skal du ta kontakt med banken og be dem sperre kortet. Banken vil i et slikt tilfelle være behjelpelig med å utstede et nytt kort.

6. *Kan den firesifrete PIN-koden leses ut av kortet?*

   Nei, kortholderens personlige kode er ikke skrevet i kortet. Det er ikke mulig å finne ut koden ved å lese magnetstripen.

7. *Kan koden beregnes ut fra kortet?*

   Data fra det enkelte kort inngår i beregning av koden. Disse dataene er imidlertid langt fra tilstrekkelige til å beregne koden ettersom de bare er en del av beregningsgrunnlaget sammen med andre data (nøkler) som bankene eier. Det er ikke mulig for noen å beregne kode ut fra stripeinnholdet i et kort.

8. *Kan noen i bankene se koden min?*

   Nei, bankene har ikke kodene lagret i lesbar form.

   Også den PIN-koden som du taster inn på en terminal eller en minibank, vil være kryptert hele veien fra tastaturet og inn til sikkerhetsmodulen i banken slik at koden ikke vil være synlig for mennesker.

9. *Er det mulig at uvedkommende kan fange opp den firesifrete koden når jeg taster den inn på en terminal eller en automat?*

   Det er nedlagt et betydelig arbeid i å beskytte signaler fra terminaler og minibanker mot innsyn eller avlytting. Verken banker eller andre aktører kan bruke utstyr hvor sikkerheten ikke er blitt

typegodkjent, til håndtering av personlige koder.

Imidlertid kan det være mulig at inntasting av PIN blir observert. Mange terminaler er nå utstyrt med deksler som beskytter mot omkringstående personer som forsøker å observere koder, og forbedring av denne sikkerheten er en kontinuerlig prosess. Uansett må den enkelte kunde være oppmerksom og forsiktig og selv bidra til at ikke andre kan oppfatte koden.

10. *Har alle i Norge en unik PIN-kode?*

    Nei, det lar seg ikke gjøre. Ettersom det bare er 10000 mulige PIN-koder og det er utstedt over tre millioner bankkort vil det naturligvis være mange som har fått utdelt samme PIN. PIN-kodene er laget på en slik måte at alle PIN-koder skal være like sannsynlige for alle kortnummer slik at det skal være meget vanskelig for en som finner et kort å gjette seg til riktig PIN på de forsøk han /hun har til rådighet.

11. *Det har forekommet noen saker der det er benyttet kort og kode ved varekjøp eller kontantuttak, men som kortholder benekter å ha foretatt. Hvordan håndterer bankene dette?*

    Slike tilfeller vil normalt være en sak mellom kortholder og kortutstedende bank. Det er derfor den enkelte banks ansvar å uttale seg om spesielle saker. Er banken og kortholder uenige om hvorvidt kortholder har opptrådt uaktsomt, kan saken bringes inn for Bankklagenemnda.

12. *Hva gjør bankene for å sikre at kortsystemet har et høyt nok sikkerhetsnivå?*

    Arbeid med å påse at sikkerheten til enhver tid har riktig nivå pågår kontinuerlig. Det ble foretatt en betydelig oppgradering i løpet av høsten 1998 og våren 1999. Banknæringen har registrert den raske utviklingen i teknologien og hva som foregår, slik at oppgraderinger som øker banksystemets motstandsdyktighet mot denne typen angrep ytterligere, vil bli foretatt.

13. *Kortet mitt sluttet plutselig å virke. Hva kan ha skjedd?*

    Avmagnetisering av kort er et problem. Hvis kortet utsettes for magnetiske felter, kan data i magnetstripen bli slettet eller ødelagt. De fleste kort som brått blir uleselige, er avmagnetisert. I

tillegg bør kortholderne passe på at kortet ikke blir utsatt for sterk varme eller sollys. Bøyde eller tilsmussede kort kan også fort bli uleselige. Generelt bør kort behandles forsiktig som andre verdigjenstander!

14. *Noe må ha skjedd med kortet. I stedet for å taste PIN må jeg signere på kvitteringer. Hva kan ha skjedd?*

    Høyst sannsynlig er spor 3 i kortet blitt avmagnetisert eller blitt uleselig på annen måte. Imidlertid kan det hende at den internasjonale delen av kortet (f. eks. Visa eller Europay) fortsatt lar seg lese, og betalingsterminalene vil dermed benytte denne.

    Det anbefales at du tar kontakt med banken.

15. *Hvorfor får jeg ikke kortet mitt tilbake når det er blitt slukt?*

    Det er kortutstedende bank som bestemmer om et slukt kort skal utleveres til kortholder eller ikke. Når minibanken eies av en annen bank enn kortutstedende bank, har ikke automateiende bank lov til å gi kortet tilbake. Samarbeidsavtalene mellom bankene forutsetter at kortet skal sendes til utstederbank for at denne skal foreta undersøkelse rundt det.

16. *Hva gjør jeg hvis jeg har mistanke om en uriktig belastning?*

    Du bør umiddelbart ta kontakt med banken. Banken vil ha prosedyrer for videre behandling av saken.

17. *Er det mulig å kopiere kort?*

    Ja, det er teknisk mulig å kopiere magnetstripene og dermed lage flere kopier av et gyldig kort. Både programvare og tekniske innretninger for kopiering av magnetstriper kan kjøpes i spesialbutikker. Bankene har imidlertid gode sikkerhetsrutiner slik at bruk av kopierte kort raskt blir avslørt.

18. *Er bankkort med VISA eller Mastercard like sikre som "rene" bankkort?*

    Ja, det er ingen forskjell hva gjelder bankkortet. Bankkortdelen brukes ved hjelp av den personlige koden, mens VISA eller Mastercard-delen også kan fungere papirbasert. Her henviser vi ellers til regler og retningslinjer utgitt av VISA og Mastercard.

    Av blant annet denne grunn er det også svært viktig at bankkunder kontrollerer kontoutskriftene sine og reagerer dersom det er transaksjoner de ikke kjenner igjen. Mange bankkort med VISA og Mastercard har bilde av kortinnehaver. Dette styrker sikkerheten.

19. *Hvor mange kort og terminaler finnes det egentlig i Norge, og hvor mange transaksjoner blir utført i løpet av et år?*

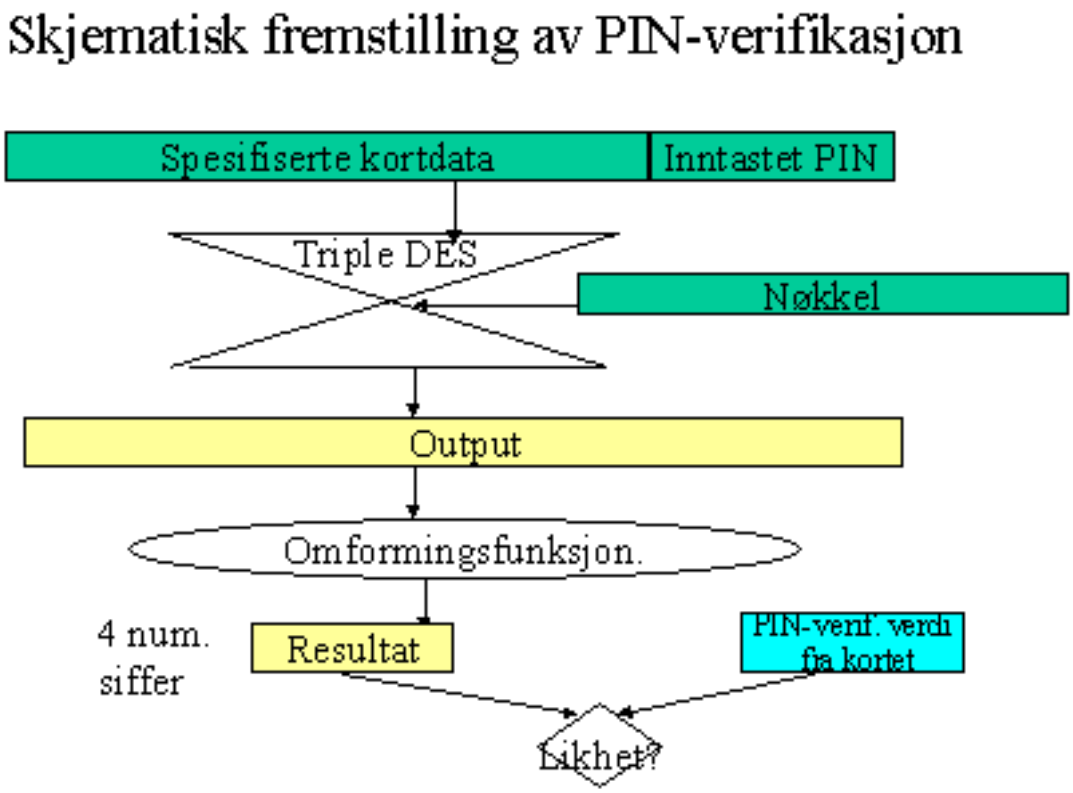
    Her henviser vil til Norges Banks årlige rapport om Betalingsformidling. Denne er lagt ut på Internett.

20. *Kan jeg bruke bankkort på nettet?*

    Det er ikke utviklet noen nasjonal løsning for elektronisk handel over Internett. Hvis kortet ditt også har en VISA eller Eurocard / Mastercard logo, vil du kunne handle på nettet etter de regler som gjelder for denne delen av ditt kort. Også her henviser vi til retningslinjer fra Visa og Europay / Mastercard. Imidlertid vil vi generelt oppfordre publikum til å være varsomme med å oppgi sitt kredittkortnummer til et ukjent firma over telefon eller Internett uten bruk av sikkerhetsfunksjoner. Da utsetter man seg for risiko for at dette nummeret kan misbrukes i andre sammenhenger.

21. *I flere andre land holder bankene på å gå over til smartkort. Vil det skje i Norge?*

    Norsk banknæring følger teknologiutviklingen nøye og vil gå over til smartkort når man finner det forretningsmessig riktig. Overgang til smartkort kan ha flere begrunnelser. I enkelte land er forbedret sikkerhet en viktig drivkraft for å introdusere smartkort. I Norge er vi imidlertid i den situasjon at vi har et on-line system som fungerer og et langt mindre utbredt kortmisbruk enn de fleste land det er naturlig å sammenligne seg med.



Tilbake igjen til hovedfremstillingen.

FYSISKE KORT

Kortene skal følge internasjonale standarder:

ISO 7810, Identification cards - Physical Characteristics.

ISO 7811, Identification cards - Recording technique.

- Part 1: Embossing

- Part 2: Magnetic stripe

- Part 3: Location of embossed characters.

- Part 4: Location of read-only magnetic cards - Tracks 1 and 2.

- Part 5: Location of read-write magnetic track - Track 3.

Disse standardene omfatter kortets størrelse, fysiske egenskaper og plassering av magnetstripen samt plassering og utforming av uthevet skrift på kortet (embossing). Det er ikke obligatorisk å ha pregedata på "bank axept"-kort. Informasjon som kan preges er navn, kortnummer og utløpsdato.

De to bankforeninger har vedtatt regler for utseende og plassering av logo på kortene. Se Avtale- og regelverksamling for innenlands betalingsformidling på www.fnh.no; Publikasjoner. Regelverket kan bestilles fra FNH.

Alle norske "bank axept"-kort skal være påført kontobanks navn på forsiden eller baksiden.

Tilbake igjen til hovedfremstillingen.

MAGNETSTRIPEN

Magnetstripen består av tre spor med informasjon:

Spor 1: 79 tegn, alfabetiske eller numeriske + spesialtegn

Spor 2: 40 tegn, numeriske + spesialtegn

Spor 3: 107 tegn, numeriske + spesialtegn.

Egenskaper for sporene (plassering, koding etc) er beskrevet i ISO-standarden 7811. For norske "bank axept"-kort brukes enten spor 2 eller spor 3 for innenlandsk betalingsformidling.

Spor 3 er laget for å kunne oppdateres løpende ved bruk slik at bankene kan godkjenne (autorisere) transaksjoner for hverandre selv uten on-line kontakt med kontobank.

Bruk av spor 2 stiller krav om on-line forbindelse med kontobank. Det nasjonale kortsystemet har utviklet seg slik at det har en meget høy on-line prosent både for spor 3 og spor 2.

Spor 1:

Internasjonal standard for spor 1: ISO 7813

Spor 1 inngår ikke i reglene for utstedelse og bruk av "bank axept"-kort. Det vil finnes "bank axept"-kort der spor 1 har data, bl.a. et kortnummer og kortholders navn. Dette er imidlertid informasjon som tilhører en samarbeidende utsteder (f. eks. et kredittkortselskap) og ikke en norsk bank.

Spor 1 brukes også av flyselskapene, bl. a. for å skrive ut navn på billetter.

Spor 2:

De aller fleste "bank axept"-kort har data i spor 2.

De nasjonale reglene sier at for kort som har et norsk bankstandard spor 3, så skal dette prioriteres fremfor spor 2 ved innenlands bruk. I spor 2 vil det derfor ofte ligge data til internasjonal bruk og som tilhører en samarbeidende utsteder (f. eks. et kredittkortselskap).

Noen banker bruker spor 2 kort som "bank axept"-kort. Utstedere av slike er bl. a. DnB - Postbanken, Sparebanken NOR (som også utsteder spor 3) og GE Capital Bank.

Internasjonal standard for spor 1: ISO 7813. Norske banker følger denne.

Informasjonsinnholdet i spor 2 kort:

Beskrivelse
Startmerke
Kortnummer
Felter disponert av kortutstedende bank.
Servicekode, angir bruksområde
Utløpsdato
Verdier relatert til PIN-verifikasjon
Feltseparator(er)
Sluttmerke
Sjekksum

Kortnummer for spor 2 administreres av internasjonale standardiseringsorganisasjoner. I Norge er det Norges Standardiseringsforbund som har ansvaret for å dele ut kortnummer.

Regler for tildeling av kortnummer finnes i standarden ISO 7812.

Spor 3:

Mesteparten av "bank axept"-kort har norske bankdata i spor 3.

Internasjonal standard for spor 3: ISO 4909. Den nasjonale norske bankstandarden avviker fra ISO 4909 på en del punkter.

Norsk bankstandard spor 3 inneholder følgende type informasjon:

Beskrivelse
Felter som identifiserer kortet og kortholder
Formatkode, identifiserer korttype
Data om bank og datasentraltilknytning
Kontonummer eller kortnummer
Kortets versjonsnummer, brukes hvis det er flere kort på en konto
Utløpsdato
Døråpnerfelt
Felter for begrensning av bruk og kontroll av aktivitet
Servicekode, angir bruksområde
Startdato og lengde for periode
Valuta eksponent
Disponibelt beløp pr. periode
Gjenværende beløp i inneværende periode
PIN forsøksteller

Sikkerhetsfelter
CSN, sikkerhetsverdi for verifikasjon av magnetstripen
Verdier relatert til PIN-verifikasjon
Felter disponert av kortutstedende bank.
Innhold kan bestemmes av den enkelte bank

Tilbake igjen til hovedfremstillingen.

KONTROLLER

Som en del av godkjennelsen av en transaksjon foretas alltid følgende kontroller ved uttak i minibank eller kjøp av varer / tjenester på terminal på brukersted:

- Kortkontroller
- Sperrekontroller
- Kontroll av kryptografiske verdier, inkl. kontroll av PIN
- Aktivitetskontroller
- Beløpskontroller

Kortkontroller (spor 3) og (spor 2):

For spor 3 kort skal bl.a. følgende kontroller utføres:

- Formatkode og data om bank og korttype skal være gyldige.
- Kontonummer / kortnummer skal ha gyldig format.
- Servicekode skal tillate den type tjeneste som er ønsket utført.
- Felter spesifisert som numeriske, skal ha numeriske verdier.
- Periodestart, periodelengde og PIN forsøksteller skal ha verdier innenfor godkjent område.
- Kortet skal ikke være utløpt.
- Sikkerhetsverdier skal være korrekt plassert.

Ved negativt resultat på en eller flere av disse kontrollene skal kortet avvises.

For spor 2 kort skal bl.a. følgende kontroller utføres:

- Feltseparatorer og markører skal stå på de riktige stedene.
- Kortnummeret skal ha gyldig format.
- Kortet skal ikke være utløpt.
- Servicekode skal tillate den type tjeneste som er ønsket utført.

Ved negativt resultat på en eller flere av disse kontrollene skal kortet avvises.

Sperrekontroller

Før en transaksjon tillates utført, skal det alltid være kontrollert mot komplett sperreliste for "bank axept"-kort.

Hvis kortet står på sperrelisten, skal det avvises. Hvis et kort som står på sperrelisten er forsøkt brukt på en automat som kan inndra kort, skal kortet beholdes av automaten.

Kontroll av kryptografiske verdier, inkl. kontroll av PIN

Det er obligatorisk å kontrollere PIN ved bruk av "bank axept"-kort.

Som hovedregel har en kortholder fire forsøk på å taste PIN. Etter fjerde feil PIN blokkeres kortet.

Hvis kortholder ikke oppgir riktig PIN, skal transaksjonen avvises. Hvis det er oppgitt fire feil PIN i automater som kan inndra kort, skal kortet beholdes av automaten.

Kortene inneholder kryptografiske verdier som skal bevise at det er et ekte kort, og at kortet ikke har vært urettmessig endret (manipulert). Dersom disse verdiene i kortet er feil eller er slettet, skal transaksjonen avvises. Automater som kan inndra kort, skal beholde kortet.

Aktivitetskontroll

Formålet med aktivitetskontroll er i hovedsak å hindre at en kortholder går ut over de beløpsgrenser som kontobank har satt for kortet.

For spor 3 kort brukes aktivitetskontroll også til å avdekke kopierte eller forfalskede kort.

Alle banker eller datasentraler som har lov til å godkjenne transaksjoner på vegne av kontobank, er forpliktet til å ha et register med aktivitetsdata.

For alle kort skal det testes på at kortholder ikke går ut over tillatte beløpsgrenser, for enkelttransaksjoner og for en gitt periode. Går kortbruken ut over beløpsgrensene, skal transaksjonen avvises.

Beløpsgrensene vil være fastsatt av kontobank. Det skal alltid testes på aktivitet og beløpsgrenser når en annen bank eller datasentral foretar autorisasjon på vegne av kontobank.

For enkelte terminaltyper og brukersteder (f. eks. på noen bensinstasjoner) er det fastsatt egne samordnede beløpsgrenser for enkelttransaksjoner eller for aktivitet pr. periode. For slike terminaler gjelder samordnede beløpsgrenser også i de tilfeller der autorisasjon har vært foretatt av kontobank.

For spor 3 kort skal det i tillegg foretas tester der data i aktivitetsregisteret blir sammenliknet med verdier i magnetstripen. Dersom verdiene i magnetstripen tilsier at kortet er manipulert, skal transaksjonen avvises. Kortet skal inndras i automater som er i stand til å gjøre det.

Beløpskontroll

Kontobank kontrollerer at det ønskede beløp for uttak eller varekjøp ikke overstiger det som kortholder har disponibelt på konto.

Tilbake igjen til hovedfremstillingen.