



FK|Finanssialan Keskusliitto  
FC|Finansbranschens Centralförbund  
Federation of Finnish Financial Services

---

# BANKERNAS EMV- BETALTERMINALSYSTEM FUNKTIONELL BESKRIVNING

21.10.2011 / V 4.2



## Innehåll:

1.	INLEDNING .....	3
2.	BEGREPP .....	4
3.	BETALTERMINALSYSTEMET .....	7
4.	AVTAL OCH GODKÄNDA KORT .....	7
5.	IDENTIFIERING OCH KONTROLL AV KORTENS ÄKTHET .....	8
6.	BETALNINGS- OCH KONTANTUTTAGSTRANSAKTIONER .....	9
6.1.	Betalningstransaktioner .....	9
6.1.1.	Avvikande situationer .....	9
6.2.	Kontantuttag med bankkort.....	10
6.3.	Cashback med Visa- och Mastercard-kort.....	10
6.5.	Betalningsmottagarens verifikat.....	11
7.	AUKTORISERING.....	11
7.1	Automatisk auktorisering .....	11
7.2	Manuell auktorisering.....	12
8	FÖRMEDLING AV VARNINGSUPPGIFTER.....	12
9	FÖRMEDLING AV TRANSAKTIONER .....	12
9.1	Principer för förmedling av transaktioner.....	12
9.2	Sändning av transaktioner .....	13
9.3	Kontroll av bankkortstransaktioner.....	13
10	KREDITERING AV BETALNINGSMOTTAGARENS KONTO.....	13
11	BEVAKNING AV KORTBETALNINGAR.....	14
13	REKLAMATION AV TRANSAKTIONER.....	17
14	AVVIKANDE SITUATIONER VID SÄNDNING AV TRANSAKTIONER .....	17
14.1	Behandling av gamla bankkortstransaktioner .....	17
14.1.1	Transaktioner äldre än 20 dagar, men nyare än 3 månader.....	17
14.1.2	Transaktioner äldre än 3 månader .....	17
14.1.3	Transaktioner som är äldre än 12 månader, men högst 3 år gamla.....	17
14.2	Övriga kort.....	18
14.3	Korrigerigering av redovisningsposter.....	18
15	SÄKERHET .....	18
15.1	PCI-krav .....	18
15.2	Anvisningar till köpmän .....	18
15.3	Bruket av personlig kod.....	18
15.4	Kryptering av datakommunikation .....	18
15.5	Förvaring av uppgifter.....	19
15.6	Radering av uppgifter.....	19
16	YTTERLIGARE INFORMATION.....	19

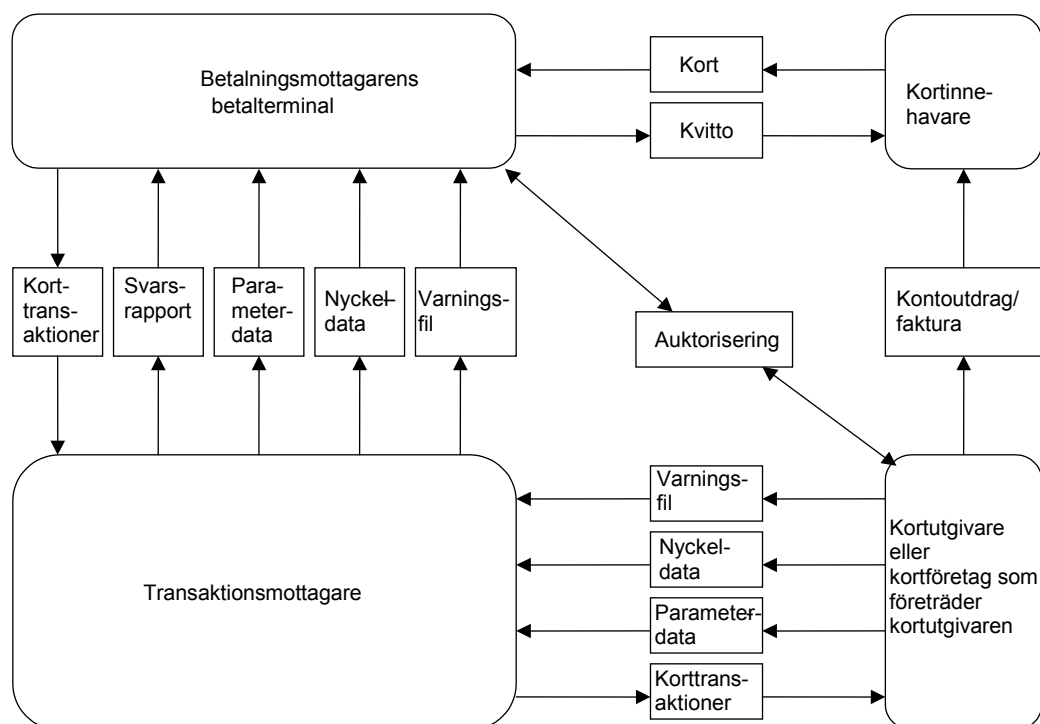
## 1. INLEDNING

Denna funktionsbeskrivning är avsedd som en bilaga till betalterminalavtalet och beskriver de allmänna principerna för bankernas EMV-betalterminalsystem.

Den här beskrivningen fokuserar på hantering av bankkortstransaktioner. Dessutom har varje kortföretag sina egna kortvillkor, vilka ska tillämpas vid behandling av transaktioner med dessa kort.

Bankernas EMV-betalterminalsystem innefattar bl.a. följande funktioner och egenskaper:

- betalnings- och kontantuttagstransaktioner samt förmedling av dessa
- auktorisering via betalterminal
- svarsrapporter samt kreditering av betalningsmottagarens konto
- förmedling av nyckel- och parameterdata
- förmedlingsrutiner för varningsuppgifter



Betaltalningsmottagaren ska följa transaktionsmottagarens och kortutfärdarnas anvisningar, avtal och säkerhetsbestämmelser.

I fråga om bankkort beskrivs ansvaret mellan banken och betaltalningsmottagaren i villkoren för bankkortsgarantin och i betaltalningsavtalet.

Vilka egenskaper som krävs av användarnas betaltalningsystem och -utrustning beskrivs i specifikationen för bankernas EMV-betalterminalsystem, vilken lämnats till berörda programvaruleverantörer.



## 2. BEGREPP

**Auktorisering** innebär att betalningsmottagaren begär tillstånd till att genomföra köpet enligt kortvillkoren, varefter kortutgivaren ser till att reservera täckning för transaktionen.

**Auktoriseringskod** är den kod som kortutgivaren ger en auktoriserad transaktion. Koden fogas till betalningsmeddelandet eller skrivs på inköpskvittot.

**Auktoriseringstjänst** används av betalningsmottagaren för att enligt kortvillkoren kontrollera kortuppgifterna och att det till kortet knutna kontot har tillräckliga medel för betalning av varan eller tjänsten eller för kontantuttaget samt för att göra en täckningsreservering. Auktoriseringen görs automatiskt via betalterminalen eller per telefon.

**Bankkort** är ett betalkort för nationellt bruk. Kortet är knutet till kundens konto i den utfärdande banken och det kan användas inom hemlandet för att betala inköp i affärer och göra kontantuttag. Nätbetalningar kan inte göras med bankkort.

**Bankkortsgarantin** innebär att banken betalar betalningsbeloppet till betalningsmottagaren då betalningsmottagaren har handlat enligt vid tillfället rådande bankgarantivillkor. Bankkortsgarantin omfattar inte kontantuttag vid kassan.

**Betalkort** är den allmänna benämningen för bankkort, kreditkort, kombinationskort och kort med betalningstid.

**Betalningsapplikation** är lagrad information i chipet på ett betalkort. Applikationen innehåller kortets betalningsegenskap (t.ex. Visa Credit, Debit MasterCard m.fl.) och regler för dess behandling, såsom de behandlingsregler som bankerna eller kortföretaget uppställt för betalterminal- eller automatanvändning. Utöver de gemensamma behandlingsreglerna kan betalningsapplikationen på chipet innehålla användningsbegränsningar och riskhanteringsparametrar som kortgivaren definierat.

**Betalningsmottagaren** som erbjuder produkter och tjänster ska ha giltiga avtal med sin kontobank om godkännande och förmedling av bankkortstransaktioner till banken (betalterminalavtal) och för övriga kort med respektive kortföretag.

**Betalterminal** se **EMV-betalterminalsystem**

**Cashback** är ett kontantuttag vid butikskassan i samband med debit- eller kreditkortköp. En cashbacktransaktion kan inte göras utan köp (jfr kontantuttag med bankkort vid butikskassan)

**Certifikat** är en komponent som används vid PKI-kryptering. Parterna identifierar varandra och TCP/IP-förbindelsen krypteras med ett certifikat som bankernas certifikattjänst tillhandahåller. EMV-kortens autenticitet bekräftas genom certifikat som utfärdats av Visa/MasterCard. DDA-korten har dessutom kortutgivarens eget certifikat.

**Chipkort** (Integrated Circuit Card, IC Card, Smart Card, Chip Card) är ett plastkort försett med en säkerhetsprocessor (chip) och dess minne. Chipet innehåller en eller flera EMV-betalningsapplikationer som används av betalterminalen. Därutöver kan chipet innehålla andra applikationer (t.ex. för identifiering eller kortkontanter). Reglerna i det gemensamma eurobetalningsområdet förutsätter att universalbetalkorten har chip enligt EMV-standarden.



**Credit-kort** (kreditkort) används för betalning av varor och tjänster från kredit som beviljats kortinnehavaren. Kreditkortet kan vara antingen universalkreditkort eller specialkreditkort. Om krediten är räntefri och köpen betalas i sin helhet per faktureringsgång kan kreditkortet också kallas för betaltidskort.

**Universalkreditkort** är ett kort som innehavaren kan använda på försäljningsställen som accepterar kortet, utan någon branschbegränsning. Specialkreditkort är ett kort som kan användas bara på vissa försäljningsställen.

**Debit-kort** är ett chipförsatt betalkort som är knutet till ett bankkonto och avsett för internationellt bruk. Debitkortet kan förutsätta online-auktorisering varje gång det används (t.ex. Visa, Electron/Maestro) eller det kan fungera så att auktorisering utförs bara vid behov, när kortets eller betalterminalens parametrar så kräver.

**EMV** är en standard för betalning med chipkort som utvecklats av de internationella kreditkortsföretagen MasterCard och Visa.

**EMV-betalterminalsystem** består av utrustning som automatiserar hämtning av nyckel- och parameterdata, betalning med kort, kontroll av spärrdata, sändning av transaktioner till banken och auktorisering av transaktioner. Utrustningen installeras hos betalningsmottagaren och ska vara certifierad av ett organ som godkänts av kortinlösaren. Betalterminalen läser av kortinformationen antingen från kortets chip eller magnetspår, gör nödvändiga kontroller, registrerar köpet och skickar transaktionen till banken.

**Kombinationskort** innehåller två eller flera betalningsapplikationer. Sådana här är t.ex. kombinationskortet bankkort/Visa-kreditkort och MasterCard Credit/Debit.

**Kontantuttag** är ett uttag av kontanter som görs med bankkort vid kassa och inte förutsätter köp (jfr cashback).

**Kortdragare** är en avtrycksapparat med vilken det präglade betalkortets och betalningsmottagarens uppgifter överförs på betalningsblanketten. På kortdragaren finns betalningsmottagarens avtalsnummer eller FO-nummer, namn, adress (och kontonummer) i reliefbokstäver. Anvisningar om användning av kortdragare ges av banker som tar emot bankkortstransaktioner eller av kortinlösare.

**Kortinlösare** (Acquirer)

Betalningsmottagaren (företaget) avtalar med en kortinlösare om kreditering av korttransaktioner samt mottagning och behandling av material (betalningstransaktioner samt varnings-, nyckel- och parameterdata). Kortutgivaren (issuer) fastställer vilken router som används för auktorisering. Inlösaren eller en av inlösaren befullmäktigad instans certifierar betalterminalerna. Inlösaren kan avtala om förmedling av transaktioner via router.

**Kortutgivare** (Issuer) är en bank eller annan sammanslutning som utfärdar kort och svarar för kortens distribution och livscykel samt för att köp och kontantuttag som gjorts med korten debiteras kortinnehavarens konto. Kortutgivaren definierar bruksvillkoren för sina kort.

**Nyckeldata** används av betalterminalen för att kontrollera att chipkortet är äkta.

**Online-auktorisering** används för att i realtid kontrollera hos kortutgivaren att kortet är giltigt.



**Parameterdata** används av EMV-terminalen för att identifiera godkända betalkort.

**PCI-säkerhetsstandarderna** har utarbetats av de internationella kortorganisationerna (American Express, Discover Financial Services, JCB International, MasterCard Worldwide och Visa Inc.) för att skydda betalkortsdata. Standarderna omfattar tekniska och funktionella krav. I PCI-standarderna ingår PCI Data Security Standard (PCI DSS), PIN Transaction Security Requirements (PCI PTS) och Payment Application Data Security Standard (PA-DSS). Mera information om säkerhetsstandarderna kan man få från PCI Security Standards Councils webbplats eller sin kortinlösare (acquirer).

**PA-DSS** (Payment Application Data Security Standard) är en säkerhetsstandard för betalprogramvara för betalning med kort, riktad särskilt till programvarutillverkare.

**PCI/DSS** (Payment Card Industry/Data Security Standard) är en säkerhetsstandard för alla parter som hanterar betalkortsdata.

**PCI PTS** (Payment Transaction Security Requirements) är en säkerhetsstandard som berör alla tillverkare av apparater för inmatning av personlig PIN-kod.

**PIN** (Personal Identification Number) är den personliga kod för kortet som bara kortinnehavaren känner till. PIN-koden kontrolleras i kontantautomater och betalterminaler för att säkerställa att den som använder kortet är den rätta kortinnehavaren. PIN används också för att godkänna betalningar.

**PIN-pad** är det lilla tangentbord som används då man knappar in PIN-koden.

**Quasi-Cash**-transaktion innebär försäljning av varor/tjänster som direkt kan bytas till kontanter, t.ex. spelrättigheter och spelmarker, valutaköp m.m.

**Referensnummer** kan användas av betalningsmottagaren för att automatisera övervakningen av kreditering. Betalningsmottagaren avtalar om användning av referens med banken, kortföretaget och utrustningsleverantören.

**Routern** förmedlar auktoriseringsbegäran från betalterminalen vidare till respektive kortutgivare och betalningstransaktionerna till transaktionsmottagaren eller kortinlösaren (acquirer). Auktoriseringen förmedlas tillbaka till betalningsmottagaren. Samma transaktion kan gå via flera routrar. Det är också möjligt att router inte alls används.

**Surcharge** är en tilläggsavgift som betalningsmottagaren tar upp.

**TCP/IP** (Transmission Control Protocol/Internet Protocol) är det protokoll som används för Internet-kommunikation.

**Transaktionsmottagare** är den som tar emot korttransaktioner och förmedlar nödvändiga filer till betalningsmottagarens betalterminal. Transaktionsmottagaren är vanligen en bank men kan också vara en tjänsteleverantör eller kortinlösare (se Kortinlösare (Acquirer)).

**Varningsfiler** innehåller uppgifter om spärrade betalkort. Filerna sänds i elektronisk form till betalterminalen.

**Varningslistor** skrivs ut på papper och innehåller uppgifter om spärrade kort. Listorna används för kontroll vid användning av kortdragare i samband med kortbetalningar

### **3. BETALTERMINALSYSTEMET**

Finansbranschens Centralförbund upprätthåller en specifikation av bankernas EMV-betalterminalsystem som definierar funktionerna i systemet.

EMV-betalterminaler och betalterminalsystem som används i Finland måste vara certifierade av ett organ med auktorisation från Finansbranschens Centralförbund. I fråga om Visa- och MasterCardkort kan betalningsmottagare få information om certifierad utrustning på Luottokuntas webbplats ([www.luottokunta.fi](http://www.luottokunta.fi)).

Betalningsmottagarna bör vända sig till en programvaru- eller utrustningsleverantör för att skaffa en EMV-betalterminal eller ett EMV-betalterminalsystem med

- kortläsare för kort med chip eller magnetremsa
- PIN-tangentbord (PIN-pad)
- display
- tangentbord
- kvittoskrivare
- betalterminalprogramvara
- dataförbindelse (för sändning och auktorisering av transaktioner)

Detaljerade bruksanvisningar för betalterminalen eller betalterminalsystemet tillhandahålls av utrustnings- eller programvarutillverkaren.

### **4. AVTAL OCH GODKÄNDA KORT**

Betalningsmottagaren ska ha ett avtal med sin kontoförande bank om:

- betalterminalservice
- godkännande av bankkort som betalningsmedel
- och vid behov ett avtal om kontantuttagsservice.

Avtalet om betalterminalservice omfattar förmedling och auktorisering av betalkortstransaktioner, uppdatering av varningsuppgifter, nyckel- och parameterdata samt svarsrapporter.

Avtalet om godkännande av bankkort som betalningsmedel omfattar alla bankkort som beviljas av finländska banker. För godkännande av övriga betalkort träffar betalningsmottagaren ett avtal med respektive kortföretag. Varje kortföretag anger sina egna villkor och anvisningar.

Kombinationskortet har förutom bankkortsapplikationen en betalkortsapplikation för internationellt bruk. Dessutom tillhandahåller bankerna partnerkort, s.k. co-branding-kort, till sina kunder i samarbete med vissa företag. Dessa kort fungerar som företagets betalkort förutom att de är bankkort eller har någon annan kortegenskap. För bankkortsegenskapen tillämpas villkoren för bankkortsgarantin och ovan nämnda anvisningar.

Avtal om auktorisering och datatrafik måste träffas med banken, teleoperatören eller någon annan serviceleverantör.

Betalningsmottagaren måste följa gällande villkor och anvisningar för betalkortet.



Finansbranschens Centralförbunds kortbetalningssektion beslutar om vilka kort som godkänns i bankernas betalterminalsystem. För systemens programvaruleverantörer tillhandahåller Finansbranschens Centralförbund en förteckning (s.k. korttavla) över de kort som duger i finländska betalterminaler.

Om betalningsmottagaren gett ut icke godkända kort till sina kunder kan denne komma överens med tillverkaren av betalterminalprogramvaran om en programändring så att även dessa kort godtas i betalningsmottagarens betalterminalsystem.

## 5. IDENTIFIERING OCH KONTROLL AV KORTENS ÄKTHET

På bankkortet ska bankens namn finnas liksom ordet "Pankkikortti" eller "Bankkort". Ett kombinationskort ska dessutom ha det internationella kortsystemets beteckningar.

Allt fler betalkort har ett chip. Dessa kort ska på baksidan ha ett magnetspår som reservsystem.

Kortnumret är inpräglad på kortet och de fyra första siffrorna har även tryckts på kortunderlaget.

Giltighetstiden anges i formatet mån/år.

Bankkort har bokstäverna "PK" eller "BK" inpräglade medan kombinationskort kan ha ytterligare mönster inpräglade.

Kortinnehavarens namn är inpräglad på kortet och innehavarens namnteckningsprov finns på kortets baksida.



Ytterligare information om identifieringen av internationella kort kan fås från transaktionsmottagaren för Visa- och MasterCard-transaktioner och i fråga om övriga kort från respektive kortföretag.

EMV-betalterminalsystemet identifierar godkända kort med hjälp av parameterdata. Chipkortens äkthet kontrolleras med hjälp nyckeldata. Det är kortutgivaren som underhåller nyckel- och parameterdata. Betalningsmottagarens bank eller någon annan transaktionsmottagare tillhandahåller materialet. Nya data hämtas automatiskt av betalterminalsystemet.

Betalningsmottagaren måste kontakta programvaru-/utrustningsleverantören när denne träffar ett avtal om godkännande av nya betalkort eller när avtalet med kortföretaget går ut.

När betalterminalen tas ur bruk eller betalterminalavtalet avslutas ska betalningsmottagaren meddela detta till transaktionsmottagaren och programvaru-/utrustningsleverantören.

Betalningsmottagaren svarar för att betalterminalsystemet har uppdaterade nyckel- och parameterdata.

## **6. BETALNINGS- OCH KONTANTUTTAGSTRANSAKTIONER**

### **6.1. Betalningstransaktioner**

Om ett chipkort används läses informationen i första hand från chipet. Kortinnehavaren placerar kortet i betalterminalens kortläsare, kontrollerar beloppet som kommer att debiteras från kontot, väljer betalningssätt om terminalen frågar om detta och godkänner transaktionen genom att knappa in sin personliga kod (PIN). Inmatningen av koden motsvarar förfarandet med identitetskontroll och namnteckning. Kunden får ett utskrivet kvitto på kortbetalningen.

Om betalningen görs med ett magnetkort utan chip läser man av kortet i en magnetkortsläsare. Personen vid kassan frågar kunden hur denne vill att kortet ska användas och väljer sedan önskat användningssätt, varefter kunden godkänner transaktionen genom sin underskrift. Identitetskontroll och auktorisering görs om kortets garantivillkor kräver detta eller av säkerhetsskäl.

Betalningsmottagaren ska förvara bankkortstransaktionernas betalterminalkvitton eller maskinläsbara uppgifter i minst aderton (18) månader. Betalningsmottagaren måste på begäran kostnadsfritt uppvisa ett verifikat eller en utskrift för en specifik transaktion. Verifikaten ska förvaras och förstöras på ett säkert sätt så att uppgifter inte hamnar hos obehöriga.

Andra kortföretag ger separata instruktioner om rutiner för användning av kort och förvaring av betalterminalkvitton.

Chipkortet styr betalterminalens funktioner och kortet kan ha olika begränsningar som definierats av banken eller kortinnehavaren.

#### **6.1.1. Avvikande situationer**

När kunden betalar med chipkort godkänner denne debiteringen med sin personliga kod och endast i undantagsfall genom att skriva sin namnteckning på kvittot. I det senare fallet görs även en auktorisering och personen vid kassan ska kontrollera kundens identitet och namnteckning. Transaktionen kan godkännas med en namnteckning om kunden inte minns sin personliga kod eller då den inte går att använda av något annat skäl.

Om chipet inte fungerar kan man läsa kortinformationen från kortets magnetremsa, vilken fungerar som reservsystem. Därefter godkänner kunden transaktionen genom att skriva sin namnteckning på kvittot. Kundens identitet måste kontrolleras och auktorisering görs.

Om det inte går att läsa av magnetremsan kan man knappa in kortnumret, om kortföretaget tillåter detta. Transaktionen måste då auktoriseras och dessutom ska en kortdragare användas så att det finns bevis på att kortet varit på platsen vid köptillfället.



Betalterminalkvittot häftas ihop med blanketten från kortdragaren och kunden skriver sin namnteckning på betalterminalkvittot.

Om kortet är präglat och kortutgivaren tillåter det kan en kortdragare fungera som reservsystem. Om kortdragare används måste man särskilt noggrant identifiera godkända kort och kontrollera spärllistor. Transaktionen måste alltid auktoriseras.

## 6.2. Kontantuttag med bankkort

Betalningsmottagaren kan erbjuda sina kunder möjligheten att ta ut kontanter vid kassan. För detta krävs ett avtal om kontantuttagsservice med banken. Kontantuttagsservicen förutsätter att tjänsten är tillgänglig för alla bankens bankkortskunder. Det ska vara tillåtet för kunden att endast ta ut kontanter. Betalningsmottagaren får inte kräva samtidigt inköp av varor eller tjänster.

En förutsättning för servicen är att betalterminalen kan hantera automatisk auktorisering. Ett kontantuttag ska auktoriseras oavsett uttaget belopp. Personen vid kassan ska kontrollera kundens identitet. Det är inte tillåtet att knappa in kortnumret.

Betalningsmottagaren får marknadsföra kontantuttagsservicen och debitera kunderna en avgift för tjänsten. Vid kassan ska det finnas en tydlig markering om att tjänsten tillhandahålls och att den är avgiftsbelagd. Uttaget belopp och avgiften för tjänsten måste specificeras på kontantuttagskvittot.

Om kontanterna i kassan håller på att ta slut får man neka servicen eller sänka beloppsgränsen för maximalt uttag. Kunderna ska omedelbart informeras om en tillfällig situation då betalningsmottagaren inte kan erbjuda kontantuttagsservicen.

Kontantuttagstransaktioner omfattas inte av bankkortsgarantin.

Kortinnehavarens bank fastställer uttagsgränsen för kontantuttag, maximalt belopp är 400 euro.

Banken kontrollerar betalterminalmeddelandets auktoriseringskod. Om auktoriseringskoden saknas eller är felaktig förkastas transaktionen och återförs till betalningsmottagaren.

## 6.3. Cashback med Visa- och Mastercard-kort

Cashback-transaktioner med Visa- och MasterCard-kort skiljer sig från kontantuttag med bankkort. Villkoren för cashback-transaktioner uppställs av och instruktioner för dem ges av acquirer för Visa- och Master-korten

## 6.4. Korrigering av transaktioner

En felaktig bankkortstransaktion kan korrigeras genom att man först gör en annulleringstransaktion och sedan en korrekt transaktion. Annulleringstransaktionen ska alltid avse den ursprungliga transaktionen och vara på samma belopp (s.k. motkontering). Annulleringen och den ursprungliga transaktionen ska sändas till banken i samma material. Betalterminalen får inte användas för att göra separata annulleringstransaktioner med bankkort. Detta innebär att enstaka återbetalningar måste skötas på annat sätt, t.ex. genom kontant återbetalning, presentkort eller girering från betalningsmottagarens konto till kunden.

Om den ursprungliga transaktionen har auktoriserats måste även auktoriseringen annulleras.

Kortföretagen ger anvisningar om korrigeringstransaktioner för deras kort.

#### 6.5. Betalningsmottagarens verifikat

Betalningsmottagaren ska förvara betalterminalkvitton för bankkortstransaktioner eller maskinläsbara uppgifter i minst aderton (18) månader. Betalningsmottagaren måste på bankens begäran kostnadsfritt uppvisa ett verifikat eller en utskrift för en specifik transaktion. Verifikaten ska förvaras och förstöras på ett säkert sätt så att uppgifter inte hamnar hos obehöriga.

Det går att skilja på betalningsmottagarens och kortinnehavarens kvitton med hjälp av kortnumret. Hela kortnumret skrivs ut på betalningsmottagarens exemplar medan endast de fyra sista siffrorna skrivs ut på kortinnehavarens kvitto.

## 7. AUKTORISERING

I EMV-systemet styrs betalterminalens funktioner av chipkortet, som initierar en auktoriseringsförfrågan utifrån de riskhanteringsparametrar som fastställts av kortutgivaren.

Inköp över ett visst belopp måste auktoriseras. Beloppsgränsen anges i villkoren för bankkortsgarantin. Försäljningsstället kan även begära auktorisering av belopp som ligger under den angivna gränsen eller göra detta i enstaka fall.

Alla kontantuttag med bankkort samt transaktioner med Visa Electron- och Maestrokort ska alltid auktoriseras maskinellt. För övriga kort fastställs auktoriseringsgränsen av respektive kortföretag.

Auktoriseringen ska göras på köpets totalbelopp. Om totalbeloppet ändras (t.ex. då man lämnar dricks på en restaurang) ska det ursprungliga köpet inklusive dess auktorisering annulleras, varefter en ny transaktion görs med det slutliga beloppet (inkl. en ny auktorisering).

I obemannade självbetjäningautomater (t.ex. i oljebolagens bensinautomater) måste alla bankkortstransaktioner auktoriseras automatiskt. Eftersom inköpsbeloppet inte är känt i förväg finns ett avtal om förhandsauktorisering och auktoriseringskorrigerering med oljebolagen.

### 7.1 Automatisk auktorisering

Betalterminalauktoriseringen bygger på den specifikation av EMV-betalterminalsystemet som upprätthålls av Finansbranschens Centralförbund. Vid betalterminalauktorisering används en krypterad TCP/IP-förbindelse eller ett privat paketförmedlande X.25-nät. Betalningsmottagaren bör genom utrustnings-/programvaruleverantören se till att auktoriseringsförbindelsen går direkt till den aktuella banken eller kortutgivaren.

TCP/IP-förbindelsen krypteras med en auktoriseringskod från bankernas auktoriseringstjänst, vilken kan beställas från banken.

Om betalningsmottagaren använder en utomstående serviceleverantör för auktoriseringstrafiken ska dessa sinsemellan avtala om genomförande- och ansvarsfrågor.

## 7.2 Manuell auktorisering

Om maskinell auktorisering via betalterminalen inte är möjlig ska man använda manuell auktorisering via telefon som reservsystem. Auktoriseringskoden som man får från auktoriseringstjänsten matas in i betalterminalen eller skrivs för hand på inköpskvittot. Bankkortens auktoriseringskoder har en kontrollsiffra för att upptäcka felslagningar.

Telefonnumret till auktoriseringstjänsten är 0100 3100.

## 8 FÖRMEDLING AV VARNINGSUPPGIFTER

Transaktionsmottagaren sammanställer varningsuppgifter, som hämtas av betalningsmottagarens betalterminalsystem. Uppgifterna skapas alla dagar, även under veckoslut och helger.

Finansbranschens Centralförbunds kortbetalningssektion beslutar om vilka varningsuppgifter som förmedlas i betalterminalsystemet.

Betalningsmottagaren och banken avtalar om hämtning av en varningslista på papper, vilken fungerar som reservsystem.

Varningsuppgifterna kan hämtas av betalningsmottagaren från och med klockan 00.00. Betalningsmottagaren ska hämta varningsuppgifterna innan försäljningen börjar. Om försäljningsstället inte är öppet alla dagar måste betalningsmottagaren se till att även hämta varningslistor för sådana dagar.

Betalningsmottagarens ansvar gällande varningsuppgifterna för betalkorten inträder omedelbart efter det att varningarna har hämtats, dock senast ett dygn efter det att banken tillhandahållit varningarna för avhämtning. För övriga kort definieras tidpunkten för ansvarsinträdandet av varje kortföretag.

Varje kortföretag svarar för att innehållet i varningsuppgifterna är korrekt.

## 9 FÖRMEDLING AV TRANSAKTIONER

### 9.1 Principer för förmedling av transaktioner

EMV-betalterminaler och -betalterminalsystem måste vara certifierade av ett organ som auktoriserats av Finansbranschens Centralförbund. Betalningsmottagaren svarar för att transaktionsmaterialet är korrekt samt för sändning av materialet och hämtning av svarsrapporter. Banken svarar för behandling av mottaget material, kreditering av betalningsmottagarens konto för bankkortstransaktioner, skapande av svarsrapporter samt hantering av transaktioner så att de blir tillgängliga för kortföretagen.

Bankkortet är i regel endast giltigt i Finland, men en betalterminal som certifierats i Finland kan placeras på ett finländskt företags försäljningsställe i utlandet för mottagning av finländska bank- och betalkort. Detta måste dock avtalas separat med banken som mottar transaktionerna. Bankkortstransaktioner som förmedlas från utlandet måste vara i euro. Bankkortsgarantin gäller inte för transaktioner som gjorts i utlandet. Förmedling

av andra än bankkortstransaktioner från utlandet till Finland måste avtalas separat med varje kortföretag.

Om betalningsmottagaren använder en utländsk serviceleverantör för datatrafiken ska dessa sinsemellan avtala om genomförande- och ansvarsfrågor.

## 9.2 Sändning av transaktioner

Bankerna rekommenderar att materialet sänds en gång per dygn. Bankerna tar emot transaktioner alla veckodagar 24 timmar om dygnet. Om tidsinställd sändning används bör transaktionerna sändas på andra tider än jämna klockslag för undvikande av rusning.

Bankkortstransaktioner ska sändas senast 20 dagar efter transaktionsdagen. Om det inte är möjligt att sända transaktionerna inom den ovan angivna tiden måste betalningsmottagaren omedelbart kontakta banken och berörda kortföretag.

Betalterminalsystemet skapar en sändningsrapport, som betalningsmottagaren ska kontrollera, se punkt 11.

## 9.3 Kontroll av bankkortstransaktioner

Banken är inte skyldig att godkänna transaktionen i bland annat följande situationer:

- transaktionen är äldre än 20 dagar
- betalterminalmeddelandet avviker från den gällande specifikationen för betalterminalsystemet
- kortnumrets kontrollsiffror stämmer inte
- gränser som anges i villkoren för bankkortsgarantin har inte följts
- transaktionen överskrider auktoriseringsgränsen, men auktorisering har inte gjorts eller auktoriseringskodens kontrollsiffra stämmer inte
- kontantuttagstransaktionen har inte auktoriserats
- sändningen till banken har ett datum som är äldre än 5 dagar.

För andra kort än bankkort ska man följa respektive kortutgivares villkor och anvisningar.

## 10 KREDITERING AV BETALNINGSMOTTAGARENS KONTO

När banken som mottagit transaktionerna kontrollerat materialet krediteras betalningsmottagarens konto för alla inköp och kontantuttag som gjorts med samtliga bankers bankkort. Bankkortstransaktioner som sänds till banken på en bankdag krediteras på sändningsdagen om materialet kommit banken till handa före ett angivet klockslag, i övriga fall nästa bankdag. Banken informerar om krediteringar genom svarsrapporter och kontoutdrag.

Andra typer av transaktioner än bankkortstransaktioner hanteras av banken enligt den tidtabell som avtalats med kortutgivaren eller ett kortföretag som företräder kortutgivaren. Dessa transaktioner kontrolleras av kortutgivaren. Gränser för godkännande, krediteringstidpunkt och krediteringssätt definieras i avtal mellan betalningsmottagaren och kortutgivaren.

Betalningsmottagaren kan automatisera bevakningen av krediteringar genom att använda en referens. Betalningsmottagaren avtalar med banken, kortföretaget och utrustningsleverantören om användning av referensen och dess innehåll.

## 11 BEVAKNING AV KORTBETALNINGAR

Betalningsmottagaren kan bevaka hanteringen av kortbetalningar med hjälp av sändningsrapporter samt svarsrapporter och kontoutdrag från banken.

Betalterminalens sändningsrapport visar antal och totalbelopp för sända kortbetalningar per redovisningspost och korttyp. Sändningsrapporten visar också om sändningen misslyckats.

Banken skapar en svarsrapport utifrån mottagna transaktioner där följande uppgifter finns för varje redovisad post:

- belopp som betalats in på betalningsmottagarens konto
- antal transaktioner som vidarebefordrats per kortföretag och
- specifikation av förkastade transaktioner.

Genom att jämföra sändningsrapporten och bankens svarsrapport kan betalningsmottagaren kontrollera att banken behandlat och godkänt betalningarna. Betalningsmottagaren är skyldig att kontrollera att svarsrapporten och motsvarande sändningsrapport stämmer överens med inbetalningen på kontoutdraget.

Kontoutdraget visar det godkända materialet per redovisningspost.

### Exempel på bevakning av betalningar

Betalterminalen gör en automatisk sändning klockan 1.05 natten till onsdagen. Materialet innehåller tisdagens kortförsäljning.

<b>Sändningsrapport</b>		
26.07.2006 01:05		
<b>REDOVISNINGSPOST 0001009</b>		
BANKKORT	ST	€
DEBITERING	25	1 000,00
KORRIGERING	0	0,00
=====	=====	=====
TOTALT	25	1 000,00

<b>REDOVISNINGSPOST 0001010</b>		
LUOTTOKUNTA	ST	€
DEBITERING	12	480,00
KORRIGERING	1	40,00
=====	=====	=====
TOTALT	13	440,00

- Butiken får in pengarna från tisdagens bankkortsbetalningar till sitt konto på onsdagen.

- Betalterminalen hämtar svarsrapporten klockan 1.05 natten mot torsdagen samtidigt som den sänder onsdagens transaktioner.

<b>Svarsrapport</b>		
26.7.2006 15:30		
<b>Redovisningspost 0001009</b>		
FÖRKASTAT		
KORT	0004920510032370746	
€	15,00	
K-REFERENS	960723K12T0556	
FÖRKLARING	KORTNUMMER	
BANKKORT	ST	€
DEBITERING	24	985,00
KORRIGERING	0	0,00
=====	=====	=====
TOTALT	24	985,00
<b>Redovisningspost 0001010</b>		
LUOTTOKUNTA	ST	€
DEBITERING	12	480,00
KORRIGERING	1	40,00
=====	=====	=====
TOTALT	13	440,00

- på torsdag morgon jämför butiken svarsrapporten med den sändningsrapport som betalterminalen skrev ut natten till onsdagen
- man ser att en av tisdagens kortbetalningar har förkastats vid bankens granskning och att det kommit in 15 euro mindre än beräknat på kontot
- butiken reder ut betalningstransaktionen och orsaken till felet med hjälp av köpets arkivreferens (K-REFERENS)

<b>Kontoutdrag</b>		
Betaldag Valutadag -----	Mottagare/Betalare Meddelande -----	Belopp -----
2607	OY BUTIK AB	985,00
2707	Betalterminaltjänst 0001009	
	BETALNING           24	985,00
	ST	0,00
	0 ST	

- Butiken kan därmed kvitta tisdagens bankkortsförsäljning mot sina kundfordringar minus den oklara kortbetalningen på 15 euro.

Efter några dagar syns krediteringen från Luottokunta på kontoutdraget. Kortföretagens krediteringar består av debiteringar och korrigeringar av dessa. Kortföretagens provision dras av från krediteringen.

Exempel:

Debiteringar 480,00 €  
- korrigeringar 40,00 €  
- provision x %

Butiken kan kvitta beloppet mot sina kundfordringar. Butiken och kortföretaget reder ut eventuella oklarheter rörande kortbetalningar sinsemellan.

## **12 FÖRVARING AV VERIFIKAT**

Enligt betaltjänstlagens 70 § är kundens reklamationsstid 13 månader. Det betyder att kunden har rätt att av sin bank inom 13 månader efter att kontot debiterats, kräva återbetalning av obehörig eller felaktigt genomförd transaktion. Tiden löper alltså inte från inköpsdagen, som däremot är den dag då handelsmannens skyldighet att förvara verifikatet börjar.

Eftersom reklamationsstiden på 13 månader räknas från kontodebiteringen och inte från inköpsdagen ska verifikat förvaras i minst 18 månader .

Utgående från bokföringslagstiftningen behöver betalterminalverifikat inte förvaras (enligt bokföringsnämndens mening) men verifikaten är viktiga i andra sammanhang, t.ex. vid fall av kortmissbruk och vid behandling av gamla transaktioner.

## **13 REKLAMATION AV TRANSAKTIONER**

Om kortinnehavaren eller kortinnehavarens kontoförande bank reklamerar en betalning med betalterminalavtalet och/eller villkoren för bankkortsgarantin som grund, får betalningsmottagaren debiteras för betalningen tills saken har utretts. Det slutliga beslutet fattas efter att utredningen är klar. Betalningsmottagaren är skyldig att överlämna det aktuella verifikatet eller uppgifter om transaktionen till banken utan kostnad.

## **14 AVVIKANDE SITUATIONER VID SÄNDNING AV TRANSAKTIONER**

### **14.1 Behandling av gamla bankkortstransaktioner**

Betalningsmottagare rekommenderas att enligt punkt 11 kontinuerligt följa med kortbetalningsredovisningen så att transaktionerna inte hinner bli föråldrade.

#### **14.1.1 Transaktioner äldre än 20 dagar, men nyare än 3 månader**

Om sändningen dröjer mer än 20 dagar ska betalningsmottagaren ta kontakt med sin kontoförande bank och komma överens om en tidpunkt för sändningen.

#### **14.1.2 Transaktioner äldre än 3 månader**

Om sändningen har dröjt mer än tre månader ska betalningsmottagaren ge banken en redogörelse beträffande orsaken till dröjsmålet samt uppgifter om transaktionerna för att kunna beställa kortinnehavarnas kontaktuppgifter. Betalningsmottagaren måste informera kortinnehavarna om dröjsmålet minst två veckor innan transaktionerna sänds till banken.

Banken har rätt att debitera betalningsmottagaren för kostnader som uppkommer vid hantering av de försenade transaktionerna.

#### **14.1.3 Transaktioner som är äldre än 12 månader, men högst 3 år gamla**

Banken har inte skyldighet att behandla transaktioner som är äldre än tolv månader även om betalningsmottagaren kan kräva betalning från kunden i tre år enligt lagen om

preskription av skulder. Betalningsmottagaren kan själva driva in sin fordran direkt hos betalaren.

#### 14.2 Övriga kort

För övriga kort ska man följa respektive kortföretags anvisningar.

#### 14.3 Korrigering av redovisningsposter

För att korrigera en dubbelsändning eller då hela redovisningsposten är felaktig måste betalningsmottagaren kontakta sin kontoförande bank och komma överens om sändning av en korrigeringspost.

För övriga kort ska man följa respektive kortföretags anvisningar.

### 15 SÄKERHET

#### 15.1 PCI-krav

Alla parter som tar emot, förmedlar, lagrar eller godkänner korttransaktioner måste iakttä vid tillfället gällande internationella säkerhetsstandarder, såsom PCI.

Säkerhetsstandarderna PCI DSS (Payment Card Industry Data Security Standard) är godkända av de internationella kortorganisationerna. Mer information om PCI DSS-standarderna finns tillgänglig på nätet (<https://www.pcisecuritystandards.org/>)

PCI/DSS är en teknisk standard och PA- DSS en funktionell standard.

#### 15.2 Anvisningar till köpmän

Finansbranschens Centralförbund, Luottokunta och Förbundet för Finsk Handel har i samråd utarbetat rekommendationer för att göra det lättare att välja betalterminaler och kunna placera apparaterna så ändamålsenligt som möjligt för både kunden och köpmannen. Anvisningarna till köpmän om placeringen av betalterminaler finns tillgängliga på FC:s webbplats [http://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Sirukortti\\_kauppiasohje.pdf](http://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Sirukortti_kauppiasohje.pdf) (FI/SWE).

#### 15.3 Bruket av personlig kod

Tangentbordet för inmatning av den personliga koden bör placeras så att andra inte kan se koden. De flesta tangentborden är flyttbara. Dessa går att vrida i höjd- eller sidled, vilket möjliggör en säker inmatning av koden. Vid placeringen bör man även ta hänsyn till behoven hos särskilda användargrupper.

Kassapersonalen får ge vägledning till kunderna i frågor som rör betalning med kort. Kortinnehavaren ska dock alltid knappa in sin personliga kod själv. Personen vid kassan får inte ens på begäran knappa in koden för kundens räkning.

#### 15.4 Kryptering av datakommunikation

Sändning av transaktioner ska skyddas enligt specifikationen i banksäkerhetsstandarderna PATU, som utarbetats av Finansbranschens Centralförbund. Betalningsmottagaren får nödvändiga kodnycklar från sin egen bank.



Kravet är att all datatrafik som innehåller bankmaterial krypteras vid mobil och publik internetkommunikation samt vid bruk av utländska förbindelser. Tekniken som används ska bygga på s.k. stark kryptering. Krypteringsmetoder som används i WLAN-, GSM- och GPRS-system är i sig inte tillräckliga. Krypteringen måste omfatta hela förbindelsen från början till slut.

#### 15.5 Förvaring av uppgifter

Betalningsmottagaren svarar för att uppgifter om kortbetalningar förvaras enligt PCI-kraven och att de inte hamnar hos obehöriga.

#### 15.6 Radering av uppgifter

När en betalterminal tas ur bruk ska betalningsmottagaren meddela detta till mottagaren av korttransaktionerna. I samband med urbruktagandet ska betalningsmottagaren radera alla offentliga nycklar från betalterminalen. Betalterminalen har en styrfunktion för detta.

När betalningsmottagarens avtal med kortföretaget upphör ska betalningsmottagaren radera kortföretagets offentliga nycklar från betalterminalen. Betalterminalen har en styrfunktion för detta.

### 16 YTTERLIGARE INFORMATION

Ytterligare information kan fås från Finansbranschens Centralförbunds webbplats [www.fkl.fi](http://www.fkl.fi).

Råd om valet av betalterminal och apparatens placering finns i "Anvisningar till köpmän", men utrustningsleverantören ger anvisningar om den egentliga användningen av betalterminalen.

Anvisningar om godkännande av Visa- och MasterCard-kort ges av inlösaren av korttransaktionerna (t.ex. Luottokunta) och för övriga internationella kort av respektive kortföretag.

Andra länkar:

<https://www.americanexpress.com/finland/>

<http://www.dinersclub.fi/dof/>

<http://www.luottokunta.fi>

<http://www.mastercard.com/fi/personal/fi/>

<http://www.visa.fi/fi.aspx>